

---


# Summit 300-48 Switch Software User Guide

Software Version 6.2a

Extreme Networks, Inc.  
3585 Monroe Street  
Santa Clara, California 95051  
(888) 257-3000  
<http://www.extremenetworks.com>

©2003 Extreme Networks, Inc. All rights reserved. Extreme Networks, ExtremeWare, Alpine, and BlackDiamond are registered trademarks of Extreme Networks, Inc. in the United States and certain other jurisdictions. ExtremeWare Vista, ExtremeWorks, ExtremeAssist, ExtremeAssist1, ExtremeAssist2, PartnerAssist, Extreme Standby Router Protocol, ESRP, SmartTraps, Summit, Summit1, Summit4, Summit4/FX, Summit7i, Summit24, Summit48, Summit Virtual Chassis, SummitLink, SummitGbX, SummitRPS and the Extreme Networks logo are trademarks of Extreme Networks, Inc., which may be registered or pending registration in certain jurisdictions. The Extreme Turbodrives logo is a service mark of Extreme Networks, which may be registered or pending registration in certain jurisdictions. Specifications are subject to change without notice.

NetWare and Novell are registered trademarks of Novell, Inc. Merit is a registered trademark of Merit Network, Inc. Solaris is a trademark of Sun Microsystems, Inc. F5, BIG/ip, and 3DNS are registered trademarks of F5 Networks, Inc. see/IT is a trademark of F5 Networks, Inc.

 "Data Fellows", the triangle symbol, and Data Fellows product names and symbols/logos are trademarks of Data Fellows.

 F-Secure SSH is a registered trademark of Data Fellows.

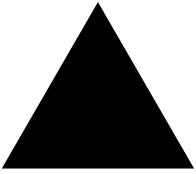
All other registered trademarks, trademarks and service marks are property of their respective owners.

Authors: Julie Laccabue, Barbara Weinstein

Editor: Amy Guzules

Production: Julie Laccabue

Special Thanks: Collin Batey, Valerie Swisher, Richard Small



# Contents

---

	<b>Preface</b>	
	<b>Introduction</b>	<b>15</b>
	<b>Conventions</b>	<b>15</b>
	<b>Related Publications</b>	<b>16</b>
<b>Chapter 1</b>	<b>ExtremeWare Overview</b>	
	<b>Summary of Features</b>	<b>17</b>
	Unified Access	18
	Virtual LANs (VLANs)	18
	Spanning Tree Protocol	18
	Quality of Service	19
	Load Sharing	19
	ESRP-Aware Switches	19
	<b>Software Licensing</b>	<b>19</b>
	<b>Security Licensing</b>	<b>20</b>
	Obtaining a Security License	20
	Security Features Under License Control	20
	<b>Software Factory Defaults</b>	<b>20</b>
<b>Chapter 2</b>	<b>Accessing the Switch</b>	
	<b>Understanding the Command Syntax</b>	<b>23</b>
	Syntax Helper	24
	Command Shortcuts	24
	Summit 300-48 Switch Numerical Ranges	24
	Names	25
	Symbols	25
	<b>Line-Editing Keys</b>	<b>25</b>
	<b>Command History</b>	<b>26</b>
	<b>Common Commands</b>	<b>26</b>

<b>Configuring Management Access</b>	<b>28</b>
User Account	29
Administrator Account	29
Default Accounts	29
Creating a Management Account	30
<b>Domain Name Service Client Services</b>	<b>31</b>
<b>Checking Basic Connectivity</b>	<b>32</b>
Ping	32
Traceroute	32
<b>Chapter 3 Managing the Switch</b>	
<b>Overview</b>	<b>35</b>
<b>Using the Console Interface</b>	<b>36</b>
<b>Using Telnet</b>	<b>36</b>
Connecting to Another Host Using Telnet	36
Configuring Switch IP Parameters	36
Disconnecting a Telnet Session	38
Controlling Telnet Access	39
<b>Using Secure Shell 2 (SSH2)</b>	<b>39</b>
Enabling SSH2 for Inbound Switch Access	39
<b>Using SNMP</b>	<b>40</b>
Accessing Switch Agents	40
Supported MIBs	41
Configuring SNMP Settings	41
Displaying SNMP Settings	42
<b>Authenticating Users</b>	<b>43</b>
RADIUS Client	43
<b>Using ExtremeWare Vista</b>	<b>47</b>
Controlling Web Access	47
Setting Up Your Browser	47
Accessing ExtremeWare Vista	48
Navigating ExtremeWare Vista	48
Saving Changes	50
Filtering Information	50
Do a GET When Configuring a VLAN	51
Sending Screen Output to Extreme Networks	51
<b>Using the Simple Network Time Protocol</b>	<b>51</b>
Configuring and Using SNTP	51
SNTP Configuration Commands	54
SNTP Example	54
<b>Chapter 4 Configuring Ports on a Switch</b>	

<b>Port Numbering</b>	<b>55</b>
<b>Enabling and Disabling Switch Ports</b>	<b>55</b>
Configuring Switch Port Speed and Duplex Setting	56
Switch Port Commands	56
<b>Load Sharing on the Switch</b>	<b>57</b>
Load-Sharing Algorithms	57
Configuring Switch Load Sharing	58
Load-Sharing Example	59
Verifying the Load-Sharing Configuration	59
<b>Switch Port-Mirroring</b>	<b>59</b>
Port-Mirroring Commands	60
Port-Mirroring Example	61
<b>Extreme Discovery Protocol</b>	<b>61</b>
EDP Commands	61
<b>Chapter 5 Virtual LANs (VLANs)</b>	
<b>Overview of Virtual LANs</b>	<b>63</b>
Benefits	63
<b>Types of VLANs</b>	<b>64</b>
Port-Based VLANs	64
Tagged VLANs	66
<b>VLAN Names</b>	<b>69</b>
Default VLAN	69
Renaming a VLAN	70
<b>Configuring VLANs on the Switch</b>	<b>70</b>
VLAN Configuration Commands	70
VLAN Configuration Examples	71
<b>Displaying VLAN Settings</b>	<b>71</b>
<b>Chapter 6 Wireless Networking</b>	
<b>Overview of Wireless Networking</b>	<b>73</b>
Summary of Wireless Features	74
<b>Wireless Devices</b>	<b>74</b>
<b>Bridging</b>	<b>75</b>
<b>Managing Wireless Ports</b>	<b>75</b>
<b>Configuring RF Properties</b>	<b>76</b>
<b>Configuring Wireless Switch Properties</b>	<b>78</b>
Configuring Country Codes	78
<b>Configuring Wireless Ports</b>	<b>79</b>

	<b>Configuring Wireless Port Interfaces</b>	<b>79</b>
	<b>Managing Wireless Clients</b>	<b>80</b>
	<b>Show Commands</b>	<b>80</b>
	<b>Event Logging and Reporting</b>	<b>81</b>
<b>Chapter 7</b>	<b>Unified Access Security</b>	
	<b>Overview of Security</b>	<b>83</b>
	<b>User Access Security</b>	<b>84</b>
	Authentication	84
	Privacy	85
	Cipher Suites	85
	<b>Network Security Policies</b>	<b>87</b>
	Policy Design	87
	Policy Examples	88
	Policies and RADIUS Support	88
	RADIUS Attributes	88
	<b>CLI Commands for Security on the Switch</b>	<b>89</b>
	Security Profile Commands	89
	<b>Example Wireless Configuration Process</b>	<b>91</b>
		93
<b>Chapter 8</b>	<b>Power Over Ethernet</b>	
	<b>Overview</b>	<b>95</b>
	Summary of PoE Features	95
	<b>Port Power Management</b>	<b>96</b>
	Port Power Operator Limit	96
	Power Budget Management	96
	Port Power Events	97
	<b>Per-Port LEDs</b>	<b>98</b>
	<b>Configuring Power Over Ethernet</b>	<b>98</b>
<b>Chapter 9</b>	<b>Forwarding Database (FDB)</b>	
	<b>Overview of the FDB</b>	<b>103</b>
	FDB Contents	103
	FDB Entry Types	103
	How FDB Entries Get Added	104
	Associating a QoS Profile with an FDB Entry	104
	<b>Configuring FDB Entries</b>	<b>105</b>
	FDB Configuration Examples	106
	<b>Displaying FDB Entries</b>	<b>106</b>

<b>Chapter 10</b>	<b>Access Policies</b>	
	<b>Overview of Access Policies</b>	<b>107</b>
	Access Control Lists	107
	Rate Limits	107
	<b>Using Access Control Lists</b>	<b>107</b>
	Access Masks	108
	Access Lists	108
	Rate Limits	109
	How Access Control Lists Work	109
	Access Mask Precedence Numbers	110
	Specifying a Default Rule	110
	The permit-established Keyword	111
	Adding Access Mask, Access List, and Rate Limit Entries	111
	Deleting Access Mask, Access List, and Rate Limit Entries	112
	Verifying Access Control List Configurations	112
	Access Control List Commands	112
	Access Control List Examples	116
<b>Chapter 11</b>	<b>Quality of Service (QoS)</b>	
	<b>Overview of Policy-Based Quality of Service</b>	<b>121</b>
	<b>Applications and Types of QoS</b>	<b>122</b>
	Voice Applications	122
	Video Applications	122
	Critical Database Applications	122
	Web Browsing Applications	123
	File Server Applications	123
	<b>Configuring QoS for a Port or VLAN</b>	<b>123</b>
	<b>Traffic Groupings</b>	<b>124</b>
	Access List Based Traffic Groupings	124
	MAC-Based Traffic Groupings	125
	Explicit Class of Service (802.1p and DiffServ) Traffic Groupings	126
	Configuring DiffServ	128
	Physical and Logical Groupings	130
	<b>Verifying Configuration and Performance</b>	<b>131</b>
	QoS Monitor	131
	Displaying QoS Profile Information	132
	<b>Modifying a QoS Configuration</b>	<b>132</b>
	<b>Traffic Rate-Limiting</b>	<b>132</b>
<b>Chapter 12</b>	<b>Status Monitoring and Statistics</b>	
	<b>Status Monitoring</b>	<b>133</b>

<b>Port Statistics</b>	<b>135</b>
<b>Port Errors</b>	<b>136</b>
<b>Port Monitoring Display Keys</b>	<b>137</b>
<b>Setting the System Recovery Level</b>	<b>137</b>
<b>Logging</b>	<b>138</b>
Local Logging	139
Remote Logging	139
Logging Configuration Changes	140
Logging Commands	140
<b>RMON</b>	<b>142</b>
About RMON	142
RMON Features of the Switch	142
Configuring RMON	143
Event Actions	144
<b>Chapter 13 Spanning Tree Protocol (STP)</b>	
<b>Overview of the Spanning Tree Protocol</b>	<b>145</b>
<b>Spanning Tree Domains</b>	<b>145</b>
Defaults	146
STPD BPDU Tunneling	146
<b>STP Configurations</b>	<b>146</b>
<b>Configuring STP on the Switch</b>	<b>148</b>
STP Configuration Example	151
<b>Displaying STP Settings</b>	<b>151</b>
<b>Disabling and Resetting STP</b>	<b>152</b>
<b>Chapter 14 IP Unicast Routing</b>	
<b>Overview of IP Unicast Routing</b>	<b>153</b>
Router Interfaces	154
Populating the Routing Table	154
<b>Proxy ARP</b>	<b>156</b>
ARP-Incapable Devices	156
Proxy ARP Between Subnets	156
<b>Relative Route Priorities</b>	<b>157</b>
<b>Configuring IP Unicast Routing</b>	<b>157</b>
Verifying the IP Unicast Routing Configuration	158
<b>IP Commands</b>	<b>158</b>
<b>Routing Configuration Example</b>	<b>162</b>
<b>Displaying Router Settings</b>	<b>163</b>

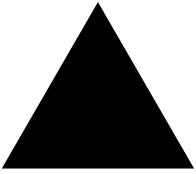


<b>Resetting and Disabling Router Settings</b>	<b>163</b>
<b>Configuring DHCP/BOOTP Relay</b>	<b>164</b>
Verifying the DHCP/BOOTP Relay Configuration	165
<b>UDP-Forwarding</b>	<b>165</b>
Configuring UDP-Forwarding	165
UDP-Forwarding Example	166
ICMP Packet Processing	166
UDP-Forwarding Commands	166
<b>Appendix A Safety Information</b>	
<b>Important Safety Information</b>	<b>169</b>
Power	169
Power Cord	170
Connections	170
Lithium Battery	171
<b>Appendix B Supported Standards</b>	
<b>Appendix C Software Upgrade and Boot Options</b>	
<b>Downloading a New Image</b>	<b>175</b>
Rebooting the Switch	176
<b>Saving Configuration Changes</b>	<b>176</b>
Returning to Factory Defaults	176
<b>Using TFTP to Upload the Configuration</b>	<b>177</b>
<b>Using TFTP to Download the Configuration</b>	<b>178</b>
Downloading a Complete Configuration	178
Downloading an Incremental Configuration	178
Scheduled Incremental Configuration Download	178
Remember to Save	179
<b>Upgrading and Accessing BootROM</b>	<b>179</b>
Upgrading Bootloader	179
Accessing the Bootstrap CLI	179
Accessing the Bootloader CLI	180
<b>Boot Option Commands</b>	<b>181</b>
<b>Appendix D Troubleshooting</b>	
<b>LEDs</b>	<b>183</b>
<b>Using the Command-Line Interface</b>	<b>184</b>
Port Configuration	185
VLANs	186
STP	187

<b>Debug Tracing</b>	<b>187</b>
<b>TOP Command</b>	<b>187</b>
<b>Contacting Extreme Technical Support</b>	<b>187</b>

**Index**

**Index of Commands**

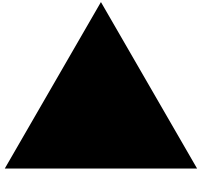


# Figures

---

<b>1</b>	Example of a port-based VLAN on the Summit 300-48 switch	64
<b>2</b>	Single port-based VLAN spanning two switches	65
<b>3</b>	Two port-based VLANs spanning two switches	66
<b>4</b>	Physical diagram of tagged and untagged traffic	68
<b>5</b>	Logical diagram of tagged and untagged traffic	68
<b>6</b>	Sample integrated wired and wireless network	74
<b>7</b>	Permit-established access list example topology	116
<b>8</b>	Access control list denies all TCP and UDP traffic	117
<b>9</b>	Access list allows TCP traffic	118
<b>10</b>	Host A initiates a TCP session to host B	118
<b>11</b>	Permit-established access list filters out SYN packet to destination	119
<b>12</b>	ICMP packets are filtered out	119
<b>13</b>	Ethernet packet encapsulation	126
<b>14</b>	IP packet header encapsulation	128
<b>15</b>	Multiple Spanning Tree Domains	147
<b>16</b>	Tag-based STP configuration	148
<b>17</b>	Routing between VLANs	154
<b>18</b>	Unicast routing configuration example	162



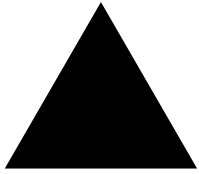


# Tables

---

<b>1</b>	Notice Icons	<b>15</b>
<b>2</b>	Text Conventions	<b>16</b>
<b>3</b>	ExtremeWare Summit 300-48 Factory Defaults	<b>20</b>
<b>4</b>	Command Syntax Symbols	<b>25</b>
<b>5</b>	Line-Editing Keys	<b>25</b>
<b>6</b>	Common Commands	<b>26</b>
<b>7</b>	Default Accounts	<b>29</b>
<b>8</b>	DNS Commands	<b>31</b>
<b>9</b>	Ping Command Parameters	<b>32</b>
<b>10</b>	SNMP Configuration Commands	<b>41</b>
<b>11</b>	RADIUS Commands	<b>43</b>
<b>12</b>	Multiselect List Box Key Definitions	<b>49</b>
<b>13</b>	Greenwich Mean Time Offsets	<b>52</b>
<b>14</b>	SNTP Configuration Commands	<b>54</b>
<b>15</b>	Switch Port Commands	<b>56</b>
<b>16</b>	Switch Port-Mirroring Configuration Commands	<b>60</b>
<b>17</b>	EDP Commands	<b>61</b>
<b>18</b>	VLAN Configuration Commands	<b>70</b>
<b>19</b>	RF Configuration Commands	<b>76</b>
<b>20</b>	RF Profile Property Values	<b>76</b>
<b>21</b>	Switch-Level Wireless Configuration Commands	<b>78</b>
<b>22</b>	Switch-Level Configuration Property Values	<b>78</b>
<b>23</b>	Wireless Port Configuration Commands	<b>79</b>
<b>24</b>	Wireless Port Configuration Property Values	<b>79</b>
<b>25</b>	Wireless Port Interface Configuration Commands	<b>80</b>
<b>26</b>	Client Configuration Commands	<b>80</b>
<b>27</b>	Show Commands	<b>80</b>
<b>28</b>	Wi-Fi Security Cipher Suites	<b>86</b>
<b>29</b>	Authentication-Based Network Access Example	<b>88</b>
<b>30</b>	RADIUS Request Attributes	<b>88</b>
<b>31</b>	RADIUS Response Attributes	<b>89</b>
<b>32</b>	Vendor-Specific Attributes	<b>89</b>
<b>33</b>	Security Profile Commands	<b>89</b>

<b>34</b>	Security Profile Command Property Values	90
<b>35</b>	Per-Port LEDs	98
<b>36</b>	Power Over Ethernet Configuration Commands	98
<b>37</b>	PoE Show Commands	101
<b>38</b>	FDB Configuration Commands	105
<b>39</b>	Access Control List Configuration Commands	113
<b>40</b>	Traffic Type and QoS Guidelines	123
<b>41</b>	QoS Configuration Commands	123
<b>42</b>	Traffic Groupings by Precedence	124
<b>43</b>	802.1p Priority Value-to-QoS Profile to Hardware Queue Default Mapping	127
<b>44</b>	802.1p Configuration Commands	127
<b>45</b>	DiffServ Configuration Commands	128
<b>46</b>	Default Code Point-to-QoS Profile Mapping	129
<b>47</b>	Status Monitoring Commands	134
<b>48</b>	Port Monitoring Display Keys	137
<b>49</b>	Fault Levels Assigned by the Switch	138
<b>50</b>	Fault Log Subsystems	138
<b>51</b>	Logging Commands	140
<b>52</b>	Event Actions	144
<b>53</b>	STP Configuration Commands	149
<b>54</b>	STP Disable and Reset Commands	152
<b>55</b>	Relative Route Priorities	157
<b>56</b>	Basic IP Commands	158
<b>57</b>	Route Table Configuration Commands	159
<b>58</b>	ICMP Configuration Commands	160
<b>59</b>	Router Show Commands	163
<b>60</b>	Router Reset and Disable Commands	163
<b>61</b>	UDP-Forwarding Commands	166
<b>62</b>	Bootstrap Command Options	180
<b>63</b>	Bootloader Command Options	180
<b>64</b>	Boot Option Commands	181



# Preface

---

This preface provides an overview of this guide, describes guide conventions, and lists other publications that may be useful.

## Introduction

This guide provides the required information to install the Summit™ 300-48 switch and configure the ExtremeWare™ software running on the Summit 300-48 switch.

This guide is intended for use by network administrators who are responsible for installing and setting up network equipment. It assumes a basic working knowledge of:

- Local area networks (LANs)
- Ethernet concepts
- Ethernet switching and bridging concepts
- Routing concepts
- Internet Protocol (IP) concepts
- Simple Network Management Protocol (SNMP)



### NOTE


---

*If the information in the release notes shipped with your switch differs from the information in this guide, follow the release notes.*



## Conventions

Table 1 and Table 2 list conventions that are used throughout this guide.

**Table 1:** Notice Icons

Icon	Notice Type	Alerts you to...
	Note	Important features or instructions.

**Table 1:** Notice Icons (continued)

Icon	Notice Type	Alerts you to...
	Caution	Risk of personal injury, system damage, or loss of data.
	Warning	Risk of severe personal injury.

**Table 2:** Text Conventions

Convention	Description
Screen displays	This typeface indicates command syntax, or represents information as it appears on the screen.
The words “enter” and “type”	When you see the word “enter” in this guide, you must type something, and then press the Return or Enter key. Do not press the Return or Enter key when an instruction simply says “type.”
[Key] names	Key names are written with brackets, such as [Return] or [Esc]. If you must press two or more keys simultaneously, the key names are linked with a plus sign (+). Example: Press [Ctrl]+[Alt]+[Del].
Words in <i>italicized type</i>	Italics emphasize a point or denote new terms at the place where they are defined in the text.

## Related Publications

The publications related to this one are:

- *ExtremeWare Release Notes*
- *Summit 300-48 Switch Release Notes*

Documentation for Extreme Networks products is available on the World Wide Web at the following location:

- <http://www.extremenetworks.com/>





# ExtremeWare Overview

---

This chapter describes the following topics:

- Summary of Features on page 17
- Security Licensing on page 20
- Software Factory Defaults on page 20

ExtremeWare is the full-featured software operating system that is designed to run on the Summit 300-48 switch. This section describes the supported ExtremeWare features for the Summit 300-48 switch.

## Summary of Features

The Summit 300-48 switch supports the following ExtremeWare features:

- Unified Access support
- Virtual local area networks (VLANs) including support for IEEE 802.1Q and IEEE 802.1p
- Spanning Tree Protocol (STP) (IEEE 802.1D)
- Quality of Service (QoS) including support for IEEE 802.1p, MAC QoS, and four hardware queues
- Wire-speed Internet Protocol (IP) forwarding
- Extreme Standby Router Protocol (ESRP) - Aware support
- Diffserv support
- Access-policy support for routing protocols
- Access list support for packet filtering
- Access list support for rate-limiting
- Load sharing on multiple ports
- RADIUS client
- Console command-line interface (CLI) connection
- Telnet CLI connection

- SSH2 connection
- Simple Network Management Protocol (SNMP) support
- Remote Monitoring (RMON)
- Traffic mirroring for ports

## Unified Access

The Summit 300-48 supports the Unified Access architecture, enabling wired and wireless applications across a completely integrated enterprise infrastructure. With the Altitude product line, the Summit 300-48 supports 802.11 WLAN connectivity. Provisioning of Unified Access is completely controlled by the Summit 300-48.

## Virtual LANs (VLANs)

ExtremeWare has a VLAN feature that enables you to construct your broadcast domains without being restricted by physical connections. A VLAN is a group of location- and topology-independent devices that communicate as if they were on the same physical local area network (LAN).

Implementing VLANs on your network has the following three advantages:

- They help to control broadcast traffic. If a device in VLAN *Marketing* transmits a broadcast frame, only VLAN *Marketing* devices receive the frame.
- They provide extra security. Devices in VLAN *Marketing* can only communicate with devices on VLAN *Sales* using routing services.
- They ease the change and movement of devices on networks.



---

For more information on VLANs, see Chapter 5, “Virtual LANs (VLANs)”.

## Spanning Tree Protocol

The Summit 300-48 supports the IEEE 802.1D Spanning Tree Protocol (STP), which is a bridge-based mechanism for providing fault tolerance on networks. STP enables you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main traffic paths fail.

A single spanning tree can span multiple VLANs.



---

For more information on STP, see Chapter 13, “Spanning Tree Protocol (STP)”.

## Quality of Service

ExtremeWare has Quality of Service (QoS) features that support IEEE 802.1p, MAC QoS, and four queues. These features enable you to specify service levels for different traffic groups. By default, all traffic is assigned the “normal” QoS policy profile. If needed, you can create other QoS policies and rate-limiting access control lists and apply them to different traffic types so that they have different maximum bandwidth, and priority.



---

*For more information on Quality of Service, see Chapter 11, “Quality of Service (QoS)”.*

## Load Sharing

Load sharing allows you to increase bandwidth and resiliency by using a group of ports to carry traffic in parallel between systems. The sharing algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see the load-sharing group as a single virtual port. The algorithm also guarantees packet sequencing between clients.



---

*For information on load sharing, see Chapter 4, “Configuring Ports on a Switch”.*

## ESRP-Aware Switches

Extreme switches that are not running ESRP, but are connected on a network that has other Extreme switches running ESRP are *ESRP-aware*. When ESRP-aware switches are attached to ESRP-enabled switches, the ESRP-aware switches reliably perform fail-over and fail-back scenarios in the prescribed recovery times. No configuration of this feature is necessary.

If Extreme switches running ESRP are connected to layer 2 switches that are not manufactured by Extreme Networks (or Extreme switches that are not running ExtremeWare 4.0 or above), the fail-over times seen for traffic local to the segment may appear longer, depending on the application involved and the FDB timer used by the other vendor’s layer 2 switch. As such, ESRP can be used with layer 2 switches from other vendors, but the recovery times vary.

The VLANs associated with the ports connecting an ESRP-aware switch to an ESRP-enabled switch must be configured using an 802.1Q tag on the connecting port, or, if only a single VLAN is involved, as untagged using the protocol filter `any`. ESRP will not function correctly if the ESRP-aware switch interconnection port is configured for a protocol-sensitive VLAN using untagged traffic.

## Software Licensing

Summit 300-48 switches support Advanced Edge licensing.

## Security Licensing

Certain additional ExtremeWare security features, such as the use of Secure Shell (SSH2) encryption, may be under United States export restriction control. Extreme Networks ships these security features in a disabled state. You can obtain information on enabling these features at no charge from Extreme Networks.

### Obtaining a Security License

To obtain information on enabling features that require export restriction, access the Extreme Networks Support website at:

<http://www.extremenetworks.com/go/security.htm>

Fill out a contact form to indicate compliance or noncompliance with the export restrictions. If you are in compliance, you will be given information that will allow you to enable security features.

### Security Features Under License Control

ExtremeWare version 6.0 and above supports the SSH2 protocol. SSH2 allows the encryption of session data. The encryption methods used are under U.S. export restriction control.

## Software Factory Defaults

Table 3 shows factory defaults for Summit 300-48 ExtremeWare features.

**Table 3:** ExtremeWare Summit 300-48 Factory Defaults

Item	Default Setting
Serial or Telnet user account	<i>admin</i> with no password and <i>user</i> with no password
Telnet	Enabled
SSH2	Disabled
SNMP	Enabled
SNMP read community string	<i>public</i>
SNMP write community string	<i>private</i>
RMON	Disabled
BOOTP	Disabled on the default VLAN ( <i>default</i> )
QoS	All traffic is part of the default queue
802.1p priority	Recognition enabled
802.3x flow control	Enabled on Gigabit Ethernet ports
Virtual LANs	Two VLANs predefined. VLAN named <i>default</i> contains all ports and belongs to the STPD named <i>s0</i> .
802.1Q tagging	All packets are untagged on the default VLAN ( <i>default</i> ).
Spanning Tree Protocol	Disabled for the switch; enabled for each port in the STPD.
Forwarding database aging period	300 seconds (5 minutes)
IP Routing	Disabled

**Table 3:** ExtremeWare Summit 300-48 Factory Defaults (continued)

<b>Item</b>	<b>Default Setting</b>
IP multicast routing	Disabled
IGMP	Enabled
IGMP snooping	Disabled
SNTP	Disabled
DNS	Disabled
Port Mirroring	Disabled
Wireless	Enabled

**NOTE**

*For default settings of individual ExtremeWare features, see the applicable individual chapters in this guide.*



# 2

## Accessing the Switch

---

This chapter describes the following topics:

- Understanding the Command Syntax on page 23
- Line-Editing Keys on page 25
- Command History on page 26
- Common Commands on page 26
- Configuring Management Access on page 28
- Domain Name Service Client Services on page 31
- Checking Basic Connectivity on page 32

### Understanding the Command Syntax

This section describes the steps to take when entering a command. Refer to the sections that follow for detailed information on using the command-line interface (CLI).

When entering a command at the prompt, ensure that you have the appropriate privilege level. Most configuration commands require you to have the administrator privilege level. To use the CLI, follow these steps:

- 1 Enter the command name.  
If the command does not include a parameter or values, skip to step 3. If the command requires more information, continue to step 2.
- 2 If the command includes a parameter, enter the parameter name and values.
- 3 The value part of the command specifies how you want the parameter to be set. Values include numerics, strings, or addresses, depending on the parameter.
- 4 After entering the complete command, press [Return].



---

*If an asterisk (\*) appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For more information on saving configuration changes, see Appendix C, “Software Upgrade and Boot Options”.*

## Syntax Helper

The CLI has a built-in syntax helper. If you are unsure of the complete syntax for a particular command, enter as much of the command as possible and press [Return]. The syntax helper provides a list of options for the remainder of the command.

The syntax helper also provides assistance if you have entered an incorrect command.

### Command Completion with Syntax Helper

ExtremeWare provides command completion by way of the [Tab] key. If you enter a partial command, pressing the [Tab] key posts a list of available options, and places the cursor at the end of the command.

### Abbreviated Syntax

Abbreviated syntax is the most unambiguous, shortest allowable abbreviation of a command or parameter. Typically, this is the first three letters of the command.

In command tables throughout this guide, abbreviated syntax is noted using bold characters.



#### NOTE

---

*When using abbreviated syntax, you must enter enough characters to make the command unambiguous and distinguishable to the switch.*

## Command Shortcuts

All named components of the switch configuration must have a unique name. Components are named using the `create` command. When you enter a command to configure a named component, you do not need to use the keyword of the component. For example, to create a VLAN, you must enter a unique VLAN name:

```
create vlan engineering
```

After you have created the VLAN with a unique name, you can then eliminate the keyword `vlan` from all other commands that require the name to be entered. For example, on the stand-alone switch, instead of entering the command

```
config vlan engineering delete port 1:1-1:3,1:6
```

you could enter the following shortcut:

```
config engineering delete port 1:1-1:3,1:6
```

## Summit 300-48 Switch Numerical Ranges

Commands that require you to enter one or more slot:port numbers on a Summit 300-48 switch use the parameter `<portlist>` in the syntax. A portlist can be a range of numbers, for example:

```
port 1:1-1:3
```

You can add additional slot and port numbers to the list, separated by a comma:

```
port 1:1-1:3, 1:6,1:8
```



## Names

All named components of the switch configuration must have a unique name. Names must begin with an alphabetical character and are delimited by whitespace, unless enclosed in quotation marks.

## Symbols

You may see a variety of symbols shown as part of the command syntax. These symbols explain how to enter the command, and you do not type them as part of the command itself. Table 4 summarizes command syntax symbols.

**Table 4:** Command Syntax Symbols

angle brackets < >	Enclose a variable or value. You must specify the variable or value. For example, in the syntax <code>config vlan &lt;name&gt; ipaddress &lt;ip_address&gt;</code> you must supply a VLAN name for <name> and an address for <ip_address> when entering the command. Do not type the angle brackets.
square brackets [ ]	Enclose a required value or list of required arguments. One or more values or arguments can be specified. For example, in the syntax <code>use image [primary   secondary]</code> you must specify either the primary or secondary image when entering the command. Do not type the square brackets.
vertical bar	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax <code>config snmp community [readonly   readwrite] &lt;string&gt;</code> you must specify either the read or write community string in the command. Do not type the vertical bar.
braces { }	Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax <code>reboot {&lt;date&gt; &lt;time&gt;   cancel}</code> you can specify either a particular date and time combination, or the keyword <code>cancel</code> to cancel a previously scheduled reboot. If you do not specify an argument, the command will prompt, asking if you want to reboot the switch now. Do not type the braces.

## Line-Editing Keys

Table 5 describes the line-editing keys available using the CLI.

**Table 5:** Line-Editing Keys

Symbol	Description
Backspace	Deletes character to left of cursor and shifts remainder of line to left.
Delete or [Ctrl] + D	Deletes character under cursor and shifts remainder of line to left.
[Ctrl] + K	Deletes characters from under cursor to end of line.
[Ctrl] + U	Clears all characters typed from cursor to beginning of line.

**Table 5:** Line-Editing Keys (continued)

Symbol	Description
[Ctrl] + W	Deletes previous word.
Insert	Toggles on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Moves cursor to left.
Right Arrow	Moves cursor to right.
Home or [Ctrl] + A	Moves cursor to first character in line.
End or [Ctrl] + E	Moves cursor to last character in line.
[Ctrl] + L	Clears screen and moves cursor to beginning of line.
[Ctrl] + P or Up Arrow	Displays previous command in command history buffer and places cursor at end of command.
[Ctrl] + N or Down Arrow	Displays next command in command history buffer and places cursor at end of command.

## Command History

ExtremeWare “remembers” the last 49 commands you entered. You can display a list of these commands by using the following command:

```
history
```

## Common Commands

Table 6 describes common commands used to manage the switch. Commands specific to a particular feature are described in the other chapters of this guide.

**Table 6:** Common Commands

Command	Description
clear session <number>	Terminates a Telnet session from the switch.
config account <username> {encrypted} {<password>}	Configures a user account password. Passwords must have a minimum of 1 character and can have a maximum of 32 characters. User names and passwords are case-sensitive.
config banner	Configures the banner string. You can enter up to 24 rows of 79-column text that is displayed before the login prompt of each session. Press [Return] at the beginning of a line to terminate the command and apply the banner. To clear the banner, press [Return] at the beginning of the first line.
config ports <portlist> auto off {speed [10   100   1000]} duplex [half   full]	Manually configures the port speed and duplex setting of one or more ports on a switch.
config ssh2 key {pregenerated}	Generates the SSH2 host key.

**Table 6:** Common Commands (continued)

Command	Description
config sys-recovery-level [none   critical   all]	<p>Configures a recovery option for instances where an exception occurs in ExtremeWare. Specify one of the following:</p> <ul style="list-style-type: none"> <li>• <code>none</code> — Recovery without system reboot.</li> <li>• <code>critical</code> — ExtremeWare logs an error to the syslog, and reboots the system after critical exceptions.</li> <li>• <code>all</code> — ExtremeWare logs an error to the syslog, and reboots the system after any exception.</li> </ul> <p>The default setting is <code>none</code>.</p>
config time <date> <time>	<p>Configures the system date and time. The format is as follows:</p> <pre>mm/dd/yyyy hh:mm:ss</pre> <p>The time uses a 24-hour clock format. You cannot set the year past 2036.</p>
config timezone <gmt_offset> {autodst   noautodst}	<p>Configures the time zone information to the configured offset from GMT time. The format of <code>gmt_offset</code> is +/- minutes from GMT time. Specify:</p> <ul style="list-style-type: none"> <li>• <code>autodst</code> — Enables automatic Daylight Savings Time change.</li> <li>• <code>noautodst</code> — Disables automatic Daylight Savings Time change.</li> </ul> <p>The default setting is <code>autodst</code>.</p>
config vlan <name> ipaddress <ip_address> {<mask>}	Configures an IP address and subnet mask for a VLAN.
create account [admin   user] <username> {encrypted} {<password>}	Creates a user account. This command is available to admin-level users and to users with RADIUS command authorization. The username is between 1 and 32 characters, the password is between 0 and 16 characters.
create vlan <name>	Creates a VLAN.
delete account <username>	Deletes a user account.
delete vlan <name>	Deletes a VLAN.
disable bootp vlan [<name>   all]	Disables BOOTP for one or more VLANs.
disable cli-config-logging	Disables logging of CLI commands to the Syslog.
disable clipaging	Disables pausing of the screen display when a show command output reaches the end of the page.
disable idletimeouts	Disables the timer that disconnects all sessions. Once disabled, console sessions remain open until the switch is rebooted or you logoff. Telnet sessions remain open until you close the Telnet client.
disable ports <portlist>	Disables a port on the switch.

**Table 6:** Common Commands (continued)

Command	Description
disable ssh2	Disables SSH2 access to the switch.
disable telnet	Disables Telnet access to the switch.
enable bootp vlan [<name>   all]	Enables BOOTP for one or more VLANs.
enable cli-config-logging	Enables the logging of CLI configuration commands to the Syslog for auditing purposes. The default setting is enabled.
enable clipaging	Enables pausing of the screen display when <code>show</code> command output reaches the end of the page. The default setting is enabled.
enable idletimeouts	Enables a timer that disconnects all sessions (both Telnet and console) after 20 minutes of inactivity. The default setting is disabled.
enable ssh2 access-profile [<name>   none] {port <tcp_port_number>}	Enables SSH2 sessions. By default, SSH2 uses TCP port number 22.
enable telnet access-profile [<name>   none] {port <tcp_port_number>}	Enables Telnet access to the switch. By default, Telnet uses TCP port number 23.
history	Displays the previous 49 commands entered on the switch.
show banner	Displays the user-configured banner.
unconfig switch {all}	Resets all switch parameters (with the exception of defined user accounts, and date and time information) to the factory defaults. If you specify the keyword <code>all</code> , the switch erases the currently selected configuration image in flash memory and reboots. As a result, all parameters are reset to default settings.

## Configuring Management Access

ExtremeWare supports the following two levels of management:

- User
- Administrator

In addition to the management levels, you can optionally use an external RADIUS server to provide CLI command authorization checking for each command. For more information on RADIUS, see “RADIUS Client” in Chapter 3, “Managing the Switch”.

## User Account

A user-level account has viewing access to all manageable parameters, with the exception of:

- User account database.
- SNMP community strings.

A user-level account can use the `ping` command to test device reachability, and change the password assigned to the account name. If you have logged on with user capabilities, the command-line prompt ends with a (>) sign. For example:

```
Summit 300-48:2>
```

## Administrator Account

An administrator-level account can view and change all switch parameters. It can also add and delete users, and change the password associated with any account name. The administrator can disconnect a management session that has been established by way of a Telnet connection. If this happens, the user logged on by way of the Telnet connection is notified that the session has been terminated.

If you have logged on with administrator capabilities, the command-line prompt ends with a (#) sign. For example:

```
Summit 300-48:18#
```

## Prompt Text

The prompt text is taken from the SNMP `sysname` setting. The number that follows the colon indicates the sequential line/command number.

If an asterisk (\*) appears in front of the command-line prompt, it indicates that you have outstanding configuration changes that have not been saved. For example:

```
*Summit 300-48:19#
```

## Default Accounts

By default, the switch is configured with two accounts, as shown in Table 7.

**Table 7:** Default Accounts

Account Name	Access Level
admin	This user can access and change all manageable parameters. The admin account cannot be deleted.
user	This user can view (but not change) all manageable parameters, with the following exceptions: <ul style="list-style-type: none"> <li>• This user cannot view the user account database.</li> <li>• This user cannot view the SNMP community strings.</li> </ul>

## Changing the Default Password

Default accounts do not have passwords assigned to them. Passwords must have a minimum of four characters and can have a maximum of 12 characters.



*User names and passwords are case-sensitive.*

To add a password to the default admin account, follow these steps:

- 1 Log in to the switch using the name *admin*.
- 2 At the password prompt, press [Return].
- 3 Add a default admin password by entering the following command:

```
config account admin
```

- 4 Enter the new password at the prompt.
- 5 Re-enter the new password at the prompt.

To add a password to the default user account, follow these steps:

- 1 Log in to the switch using the name *admin*.
- 2 At the password prompt, press [Return], or enter the password that you have configured for the *admin* account.
- 3 Add a default user password by entering the following command:

```
config account user
```

- 4 Enter the new password at the prompt.
- 5 Re-enter the new password at the prompt.



*If you forget your password while logged out of the command-line interface, contact your local technical support representative, who will advise on your next course of action.*

## Creating a Management Account

The switch can have a total of 16 management accounts. You can use the default names (*admin* and *user*), or you can create new names and passwords for the accounts. Passwords can have a minimum of 0 characters and can have a maximum of 31 characters.

To create a new account, follow these steps:

- 1 Log in to the switch as *admin*.
- 2 At the password prompt, press [Return], or enter the password that you have configured for the *admin* account.
- 3 Add a new user by using the following command:

```
create account [admin | user] <username>
```

- 4 Enter the password at the prompt.
- 5 Re-enter the password at the prompt.

## Viewing Accounts

To view the accounts that have been created, you must have administrator privileges. Use the following command to see the accounts:

```
show accounts
```

## Deleting an Account

To delete a account, you must have administrator privileges. To delete an account, use the following command:

```
delete account <username>
```



### NOTE

*The account name admin cannot be deleted.*

# Domain Name Service Client Services

The Domain Name Service (DNS) client in ExtremeWare augments the following commands to allow them to accept either IP addresses or host names:

- telnet
- download [bootrom | configuration | image]
- upload configuration
- ping
- traceroute

In addition, the `nslookup` utility can be used to return the IP address of a hostname.

Table 8 describes the commands used to configure DNS.

**Table 8:** DNS Commands

Command	Description
<code>config dns-client add &lt;ipaddress&gt;</code>	Adds a DNS name server(s) to the available server list for the DNS client. Up to three name servers can be configured.
<code>config dns-client default-domain &lt;domain_name&gt;</code>	Configures the domain that the DNS client uses if a fully qualified domain name is not entered. For example, if the default domain is configured to be <code>foo.com</code> , executing <code>ping bar</code> searches for <code>bar.foo.com</code> .
<code>config dns-client delete &lt;ipaddress&gt;</code>	Removes a DNS server.
<code>nslookup &lt;hostname&gt;</code>	Displays the IP address of the requested host.
<code>show dns-client</code>	Displays the DNS configuration.

## Checking Basic Connectivity

The switch offers the following commands for checking basic connectivity:

- ping
- traceroute

### Ping

The `ping` command enables you to send Internet Control Message Protocol (ICMP) echo messages to a remote IP device. The `ping` command is available for both the user and administrator privilege level.

The `ping` command syntax is:

```
ping {continuous} {start-size <number>} [<ip_address> | <hostname>] {from
<src_address> | with record-route | from <src_ipaddress> with record-route}
```

Options for the `ping` command are described in Table 9.

**Table 9:** Ping Command Parameters

Parameter	Description
continuous	Specifies ICMP echo messages to be sent continuously. This option can be interrupted by pressing any key.
start-size	Specifies the size of the ICMP request. If the <code>start-size</code> is specified, transmits ICMP requests using 1 byte increments, per packet.
<ipaddress>	Specifies the IP address of the host.
<hostname>	Specifies the name of the host. To use the <code>hostname</code> , you must first configure DNS.
from	Uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used.
with record-route	Decodes the list of recorded routes and displays them when the ICMP echo reply is received.

If a `ping` request fails, the switch continues to send `ping` messages until interrupted. Press any key to interrupt a `ping` request.

### Traceroute

The `traceroute` command enables you to trace the routed path between the switch and a destination endstation. The `traceroute` command syntax is:

```
traceroute [<ip_address> | <hostname>] {from <src_ipaddress>} {ttl <TTL>} {port
<port>}
```

where:

- `ip_address` is the IP address of the destination endstation.
- `hostname` is the hostname of the destination endstation. To use the `hostname`, you must first configure DNS.



- `from` uses the specified source address in the ICMP packet. If not specified, the address of the transmitting interface is used.
- `ttl` configures the switch to trace up to the time-to-live number of the switch.
- `port` uses the specified UDP port number.



# 3

## Managing the Switch

---

This chapter describes the following topics:

- Overview on page 35
- Using the Console Interface on page 36
- Using Telnet on page 36
- Using Secure Shell 2 (SSH2) on page 39
- Using SNMP on page 40
- Authenticating Users on page 43
- Using ExtremeWare Vista on page 47
- Using the Simple Network Time Protocol on page 51

### Overview

Using ExtremeWare, you can manage the switch using the following methods:

- Access the CLI by connecting a terminal (or workstation with terminal-emulation software) to the console port.
- Access the switch remotely using TCP/IP through one of the switch ports. Remote access includes:
  - Telnet using the CLI interface.
  - SSH2 using the CLI interface.
  - SNMP access using ExtremeWare Enterprise Manager or another SNMP manager.
  - Web access using ExtremeWare Vista.

The switch supports up to the following number of concurrent user sessions:

- One console session
- Eight Telnet sessions
- Eight SSH2 sessions

## Using the Console Interface

The CLI built into the switch is accessible by way of the 9-pin, RS-232 port labeled *console*, located on the front of the Summit 300-48 switch.

After the connection has been established, you will see the switch prompt and you can log in.

## Using Telnet

Any workstation with a Telnet facility should be able to communicate with the switch over a TCP/IP network.

Up to eight active Telnet sessions can access the switch concurrently. If `idletimeouts` are enabled, the Telnet connection will time out after 20 minutes of inactivity. If a connection to a Telnet session is lost inadvertently, the switch terminates the session within two hours.

Before you can start a Telnet session, you must configure the switch IP parameters. See “Configuring Switch IP Parameters” on page 36 for more information. Telnet is enabled by default.

To open the Telnet session, you must specify the IP address of the device that you want to manage. Check the user manual supplied with the Telnet facility if you are unsure of how to do this.

After the connection has been established, you will see the switch prompt and you may log in.

## Connecting to Another Host Using Telnet

You can Telnet from the current CLI session to another host using the following command:

```
telnet [<ipaddress> | <hostname>] {<port_number>}
```

If the TCP port number is not specified, the Telnet session defaults to port 23. Only VT100 emulation is supported.

## Configuring Switch IP Parameters

To manage the switch by way of a Telnet connection or by using an SNMP Network Manager, you must first configure the switch IP parameters.

### Using a BOOTP Server

If you are using IP and you have a Bootstrap Protocol (BOOTP) server set up correctly on your network, you must add the following information to the BOOTP server:

- Switch Media Access Control (MAC) address, found on the rear label of the switch
- IP address
- Subnet address mask (optional)

After this is done, the IP address and subnet mask for the switch will be downloaded automatically. You can then start managing the switch without further configuration.

You can enable BOOTP on a per-VLAN basis by using the following command:

```
enable bootp vlan [<name> | all]
```

By default, BOOTP is disabled on the *default* VLAN.

To enable the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests, use the following command:

```
enable bootprelay
```

If you configure the switch to use BOOTP, the switch IP address is not retained through a power cycle, even if the configuration has been saved. To retain the IP address through a power cycle, you must configure the IP address of the VLAN.

All VLANs within a switch that are configured to use BOOTP to get their IP address use the same MAC address. Therefore, if you are using DHCP/BOOTP relay through a router, the BOOTP server must be capable of differentiating its relay based on the gateway portion of the BOOTP packet.

### Manually Configuring the IP Settings

If you are using IP without a BOOTP server, you must enter the IP parameters for the switch in order for the SNMP Network Manager, Telnet software, or Web interface to communicate with the device. To assign IP parameters to the switch, you must perform the following tasks:

- Log in to the switch with administrator privileges.
- Assign an IP address and subnet mask to a VLAN.

The switch comes configured with a default VLAN named *default*. To use Telnet or an SNMP Network Manager, you must have at least one VLAN on the switch, and it must be assigned an IP address and subnet mask. IP addresses are always assigned to a VLAN. The switch can be assigned multiple IP addresses.



#### NOTE

---

For information on creating and configuring VLANs, see Chapter 5, “Virtual LANs (VLANs)”.

To manually configure the IP settings, follow these steps:

- 1 Connect a terminal or workstation running terminal-emulation software to the console port.
- 2 At your terminal, press [Return] one or more times until you see the login prompt.
- 3 At the login prompt, enter your user name and password. Note that they are both case-sensitive. Ensure that you have entered a user name and password with administrator privileges.
  - If you are logging in for the first time, use the default user name *admin* to log in with administrator privileges. For example:
 

```
login: admin
```

Administrator capabilities enable you to access all switch functions. The default user names have no passwords assigned.
  - If you have been assigned a user name and password with administrator privileges, enter them at the login prompt.
- 4 At the password prompt, enter the password and press [Return].

When you have successfully logged in to the switch, the command-line prompt displays the name of the switch in its prompt.

- 5 Assign an IP address and subnetwork mask for the default VLAN by using the following command:

```
config vlan <name> ipaddress <ipaddress> {<subnet_mask>}
```

For example:

```
config vlan default ipaddress 123.45.67.8 255.255.255.0
```

Your changes take effect immediately.



## NOTE

*As a general rule, when configuring any IP addresses for the switch, you can express a subnet mask by using dotted decimal notation, or by using classless inter-domain routing notation (CIDR). CIDR uses a forward slash plus the number of significant bits in the subnet mask. Using CIDR notation, the command identical to the one above would be:*

```
config vlan default ipaddress 123.45.67.8 / 24
```

- 6 Configure the default route for the switch using the following command:

```
config iproute add default <gateway> {<metric>}
```

For example:

```
config iproute add default 123.45.67.1
```

- 7 Save your configuration changes so that they will be in effect after the next switch reboot, by typing:

```
save
```

- 8 When you are finished using the facility, log out of the switch by typing:

```
logout OR quit
```

## Disconnecting a Telnet Session

An administrator-level account can disconnect a Telnet management session. If this happens, the user logged in by way of the Telnet connection is notified that the session has been terminated.

To terminate a Telnet session, follow these steps:

- 1 Log in to the switch with administrator privileges.
- 2 Determine the session number of the session you want to terminate by using the following command:

```
show session
```

- 3 Terminate the session by using the following command:

```
clear session <session_number>
```

## Controlling Telnet Access

By default, Telnet services are enabled on the switch. To display the status of Telnet, use the following command:

```
show management
```

You can choose to disable Telnet by using the following command:

```
disable telnet
```

To re-enable Telnet on the switch, at the console port use the following:

```
enable telnet
```

You must be logged in as an administrator to enable or disable Telnet.

## Using Secure Shell 2 (SSH2)

Secure Shell 2 (SSH2) is a feature of ExtremeWare that allows you to encrypt session data between the switch and a network administrator using SSH2 client software. The ExtremeWare SSH2 switch application is based on the Data Fellows™ SSH2 server implementation. It is highly recommended that you use the F-Secure® SSH client products from Data Fellows corporation. These applications are available for most operating systems. For more information, refer to the Data Fellows website at:

<http://www.datafellows.com>.



### NOTE

---

*SSH2 is compatible with the Data Fellows SSH2 client version 2.0.12 or above. SSH2 is not compatible with SSH1.*

## Enabling SSH2 for Inbound Switch Access

Because SSH2 is currently under U.S. export restrictions, you must first obtain a security-enabled version of the ExtremeWare software from Extreme Networks before you can enable SSH2. The procedure for obtaining a security-enabled version of the ExtremeWare software is described in Chapter 1.

You must enable SSH2 on the switch before you can connect to it using an external SSH2 client. Enabling SSH2 involves two steps:

- Enabling SSH2 access, which may include specifying an access profile, and specifying a TCP port to be used for communication.  
By default, if you have a security license, SSH2 is disabled using TCP port 22, with no restrictions on client access.
- Generating or specifying an authentication key for the SSH2 session.

To enable SSH2, use the following command:

```
enable ssh2 {access-profile [<access_profile> | none] {port <tcp_port_number>}}
```

You can specify a list of predefined clients that are allowed SSH2 access to the switch. To do this, you must create an access profile that contains a list of allowed IP addresses. For more information on creating access profiles, refer to Chapter 10.

You can also specify a TCP port number to be used for SSH2 communication. By default the TCP port number is 22.

The supported cipher is 3DES-CBC. The supported key exchange is DSA.

An authentication key must be generated before the switch can accept incoming SSH2 sessions. This can be done automatically by the switch, or you can enter a previously generated key. To have the key generated by the switch, use the following command:

```
config ssh2 key
```

You are prompted to enter information to be used in generating the key. The key generation process takes approximately ten minutes. Once the key has been generated, you should save your configuration to preserve the key.

To use a key that has been previously created, use the following command:

```
config ssh2 key pregenerated
```

You are prompted to enter the pregenerated key.

The key generation process generates the SSH2 private host key. The SSH2 public host key is derived from the private host key, and is automatically transmitted to the SSH2 client at the beginning of an SSH2 session.

Before you initiate a session from an SSH2 client, ensure that the client is configured for any nondefault access list or TCP port information that you have configured on the switch. Once these tasks are accomplished, you may establish an SSH2-encrypted session with the switch. Clients must have a valid user name and password on the switch in order to log into the switch after the SSH2 session has been established.

For additional information on the SSH protocol refer to [FIPS-186] Federal Information Processing Standards Publication (FIPSPUB) 186, Digital Signature Standard, 18 May 1994. This can be download from: <ftp://ftp.cs.hut.fi/pub/ssh>. General technical information is also available from:

<http://www.ssh.fi>

## Using SNMP

Any Network Manager running the Simple Network Management Protocol (SNMP) can manage the switch, provided the Management Information Base (MIB) is installed correctly on the management station. Each Network Manager provides its own user interface to the management facilities.

The following sections describe how to get started if you want to use an SNMP manager. It assumes you are already familiar with SNMP management. Extreme Networks products support SNMP v1 and SNMP v2C.

## Accessing Switch Agents

To have access to the SNMP agent residing in the switch, at least one VLAN must have an IP address assigned to it.



## Supported MIBs

In addition to private MIBs, the switch supports the standard MIBs listed in Appendix B.

## Configuring SNMP Settings

The following SNMP parameters can be configured on the switch:

- **Authorized trap receivers** — An authorized trap receiver can be one or more network management stations on your network. The switch sends SNMP traps to all trap receivers. You can have a maximum of 16 trap receivers configured for each switch. Entries in this list can also be created, modified, and deleted using the RMON2 trapDestTable MIB variable, as described in RFC 2021.
- **Community strings** — The community strings allow a simple method of authentication between the switch and the remote Network Manager. There are two types of community strings on the switch. Read community strings provide read-only access to the switch. The default read-only community string is *public*. Read-write community strings provide read and write access to the switch. The default read-write community string is *private*. A total of eight community strings can be configured on the switch. The community string for all authorized trap receivers must be configured on the switch for the trap receiver to receive switch-generated traps. SNMP community strings can contain up to 127 characters.
- **System contact** (optional) — The system contact is a text field that enables you to enter the name of the person(s) responsible for managing the switch.
- **System name** — The system name is the name that you have assigned to this switch. The default name is the model name of the switch (for example, Summit1 switch).
- **System location** (optional) — Using the system location field, you can enter an optional location for this switch.

Table 10 describes SNMP configuration commands.

**Table 10:** SNMP Configuration Commands

Command	Description
config snmp add trapreceiver <ipaddress> community <string>	Adds the IP address of a specified trap receiver. The IP address can be a unicast, multicast, or broadcast address. A maximum of 16 trap receivers is allowed.
config snmp community [readonly   readwrite] <string>	Adds an SNMP read or read/write community string. The default <i>readonly</i> community string is <i>public</i> . The default <i>readwrite</i> community string is <i>private</i> . Each community string can have a maximum of 127 characters, and can be enclosed by double quotation marks.
config snmp delete trapreceiver [<ip_address> community <string>   all]	Deletes the IP address of a specified trap receiver or all authorized trap receivers.
config snmp syscontact <string>	Configures the name of the system contact. A maximum of 255 characters is allowed.
config snmp syslocation <string>	Configures the location of the switch. A maximum of 255 characters is allowed.

**Table 10:** SNMP Configuration Commands (continued)

Command	Description
<code>config snmp sysname &lt;string&gt;</code>	Configures the name of the switch. A maximum of 32 characters is allowed. The default sysname is the model name of the device (for example, <code>Summit 300-48</code> ). The <code>sysname</code> appears in the switch prompt.
<code>disable snmp access</code>	Disables SNMP on the switch. Disabling SNMP access does not affect the SNMP configuration (for example, community strings).
<code>disable snmp traps</code>	Prevents SNMP traps from being sent from the switch. Does not clear the SNMP trap receivers that have been configured.
<code>enable snmp access</code>	Turns on SNMP support for the switch.
<code>enable snmp traps</code>	Turns on SNMP trap support.
<code>unconfig management</code>	Restores default values to all management-related entries.

## Displaying SNMP Settings

To display the SNMP settings configured on the switch, use the following command:

```
show management
```

This command displays the following information:

- Enable/disable state for Telnet, SSH2, and SNMP, and web
- SNMP community strings
- Authorized SNMP station list
- SNMP trap receiver list
- RMON polling configuration
- Login statistics
- CLI idle timeouts
- CLI paging
- CLI configuration logging

# Authenticating Users

ExtremeWare provides a Radius client to authenticate switch admin users who login to the switch:

## RADIUS Client

Remote Authentication Dial In User Service (RADIUS, RFC 2138) is a mechanism for authenticating and centrally administrating access to network nodes. The ExtremeWare RADIUS client implementation allows authentication for Telnet or console access to the switch.

You can define a primary and secondary RADIUS server for the switch to contact. When a user attempts to login using Telnet, http, or the console, the request is relayed to the primary RADIUS server, and then to the secondary RADIUS server, if the primary does not respond. If the RADIUS client is enabled, but access to the RADIUS primary or secondary server fails, the switch uses its local database for authentication.

The privileges assigned to the user (admin versus nonadmin) at the RADIUS server take precedence over the configuration in the local switch database.

## Configuring RADIUS Client

You can define primary and secondary server communication information, and for each RADIUS server, the RADIUS port number to use when talking to the RADIUS server. The default port value is 1645. The client IP address is the IP address used by the RADIUS server for communicating back to the switch.

RADIUS commands are described in Table 11.

**Table 11:** RADIUS Commands

Command	Description
<pre>config radius [primary   secondary] server [&lt;ipaddress&gt;   &lt;hostname&gt;] {&lt;udp_port&gt;} client-ip &lt;ipaddress&gt;</pre>	<p>Configures the primary and secondary RADIUS server. Specify the following:</p> <ul style="list-style-type: none"> <li>• [primary   secondary] — Configure either the primary or secondary RADIUS server.</li> <li>• [&lt;ipaddress&gt;   &lt;hostname&gt;] — The IP address or hostname of the server being configured.</li> <li>• &lt;udp_port&gt; — The UDP port to use to contact the RADIUS server. The default UDP port setting is 1645.</li> <li>• client-ip &lt;ipaddress&gt; — The IP address used by the switch to identify itself when communicating with the RADIUS server.</li> </ul> <p>The RADIUS server defined by this command is used for user name authentication and CLI command authentication.</p>
<pre>config radius [primary   secondary] shared-secret {encrypted} &lt;string&gt;</pre>	<p>Configures the authentication string used to communicate with the RADIUS server.</p>

**Table 11: RADIUS Commands (continued)**

Command	Description
show radius	Displays the current RADIUS client configuration and statistics.
unconfig radius {server [primary   secondary]}	Unconfigures the radius client configuration.

## RADIUS RFC 2138 Attributes

The RADIUS RFC 2138 optional attributes supported are as follows:

- User-Name
- User-Password
- Service-Type
- Login-IP-Host

## RADIUS Server Configuration Example (Merit)

Many implementations of RADIUS server use the publicly available Merit® AAA server application, available on the World Wide Web at:

<http://www.merit.edu/aaa>

Included below are excerpts from relevant portions of a sample Merit RADIUS server implementation. The example shows excerpts from the client and user configuration files. The client configuration file (`ClientCfg.txt`) defines the authorized source machine, source name, and access level. The user configuration file (`users`) defines username, password, and service type information.

ClientCfg.txt

```
#Client Name      Key                [type]            [version]        [prefix]
#-----
#10.1.2.3:256     test              type = nas        v2               pfx
#pm1              %^$%#*(!(*&)+    type=nas          pm1.
#pm2              :-):-(;^):-}!    type nas          pm2.
#merit.edu/homeless hmoemreilte.ses
#homeless        testing          type proxy        v1
#xyz.merit.edu    moretesting      type=Ascend:NAS v1
#anyoldthing:1234 whoknows?       type=NAS+RAD_RFC+ACCT_RFC
10.202.1.3       andrew-linux     type=nas
10.203.1.41     eric              type=nas
10.203.1.42     eric              type=nas
10.0.52.14      samf              type=nas
```

users

```
user Password = ""
  Filter-Id = "unlim"
admin Password = "", Service-Type = Administrative
  Filter-Id = "unlim"
```

```
eric    Password = "", Service-Type = Administrative
        Filter-Id = "unlim"

albert  Password = "password", Service-Type = Administrative
        Filter-Id = "unlim"

samuel  Password = "password", Service-Type = Administrative
        Filter-Id = "unlim"
```

## RADIUS Per-Command Configuration Example

Building on this example configuration, you can use RADIUS to perform per-command authentication to differentiate user capabilities. To do so, use the Extreme-modified RADIUS Merit software that is available from the Extreme Networks web server at <http://www.extremenetworks.com/extreme/support/otherapps.htm> or by contacting Extreme Networks technical support. The software is available in compiled format for Solaris™ or Linux™ operating systems, as well as in source code format. For all clients that use RADIUS per-command authentication, you must add the following type to the client file:

```
type:extreme:nas + RAD_RFC + ACCT_RFC
```

Within the `users` configuration file, additional keywords are available for `Profile-Name` and `Extreme-CLI-Authorization`. To use per-command authentication, enable the CLI authorization function and indicate a profile name for that user. If authorization is enabled without specifying a valid profile, the user is unable to perform any commands.

Next, define the desired profiles in an ASCII configuration file called `profiles`. This file contains named profiles of exact or partial strings of CLI commands. A named profile is linked with a user through the `users` file. A profile with the `permit` on keywords allows use of only the listed commands. A profile with the `deny` keyword allows use of all commands *except* the listed commands.

CLI commands can be defined easily in a hierarchal manner by using an asterisk (\*) to indicate any possible subsequent entry. The parser performs exact string matches on other text to validate commands. Commands are separated by a comma (,) or newline.

Looking at the following example content in `profiles` for the profile named `PROFILE1`, which uses the `deny` keyword, the following attributes are associated with the user of this profile:

- Cannot use any command starting with `enable`.
- Cannot issue the `disable ipforwarding` command.
- Cannot issue a `show switch` command.
- Can perform all other commands.

We know from the `users` file that this applies to the users `albert` and `lulu`. We also know that `eric` is able to log in, but is unable to perform any commands, because he has no valid profile assigned.

In `PROFILE2`, a user associated with this profile can use any `enable` command, the `clear counter` command and the `show management` command, but can perform no other functions on the switch. We also know from the `users` file that `gerald` has these capabilities.

The following lists the contents of the file `users` with support for per-command authentication:

```
user    Password = ""
```

```
Filter-Id = "unlim"

admin Password = "", Service-Type = Administrative
Filter-Id = "unlim"

eric Password = "", Service-Type = Administrative, Profile-Name = ""
Filter-Id = "unlim"
Extreme:Extreme-CLI-Authorization = Enabled

albert Password = "", Service-Type = Administrative, Profile-Name =
"Profile1"
Filter-Id = "unlim"
Extreme:Extreme-CLI-Authorization = Enabled

lulu Password = "", Service-Type = Administrative, Profile-Name =
"Profile1"
Filter-Id = "unlim"
Extreme:Extreme-CLI-Authorization = Enabled

gerald Password = "", Service-Type = Administrative, Profile-Name "Profile2"
Filter-Id = "unlim"
Extreme:Extreme-CLI-Authorization = Enabled
```

**Contents of the file "profiles":**

```
PROFILE1 deny
{
enable *, disable ipforwarding
show switch
}

PROFILE2
{
enable *, clear counters
show management
}

PROFILE3 deny
{
create vlan *, configure iproute *, disable *, show fdb
delete *, configure rip add
}
```

## Using ExtremeWare Vista

The ExtremeWare Vista™ device-management software that runs on the switch allows you to access the switch over a TCP/IP network using a standard web browser. Any properly configured standard web browser that supports frames and JavaScript (such as Netscape Navigator 3.0 or above, or Microsoft Internet Explorer 3.0 or above) can be used to manage the switch.

ExtremeWare Vista provides a subset of the command-line interface (CLI) commands available for configuring and monitoring the switch. If a particular command is not available using ExtremeWare Vista, you must use the CLI to access the desired functionality.

To use ExtremeWare Vista, at least one VLAN must be assigned an IP address.



---

*For more information on assigning an IP address, see “Configuring Switch IP Parameters” on page 36.*

The default home page of the switch can be accessed using the following command:

```
http://<ipaddress>
```

When you access the home page of the switch, you are presented with the Logon screen.

### Controlling Web Access

By default, web access is enabled on the switch. To configure Vista web access to be disabled, use the following command:

```
disable web
```

To display the status of web access, use the following command:

```
show management
```

To disable ExtremeWare Vista, use the following command:

```
disable web
```

To re-enable web access, use the `enable web` command.

By default, web access uses TCP port 80. To specify a different port, use the `port` option in the `enable web` command.



---

*For more information on rebooting, see Appendix C.*

### Setting Up Your Browser

In general, the default settings that come configured on your browser work well with ExtremeWare Vista. You can use the following recommended settings to improve the display features and functionality of ExtremeWare Vista:

- After downloading a newer version of the switch image, clear the browser disk and memory cache to see the updated menu screens. You must clear the cache while at the main ExtremeWare Vista Logon screen, so that all underlying .GIF files are updated.

- Check for newer versions of stored pages. Every visit to the page should be selected as a cache setting.

If you are using Netscape Navigator, configure the cache option to check for changes “Every Time” you request a page.

If you are using Microsoft Internet Explorer, configure the Temporary Internet Files setting to check for newer versions of stored pages by selecting “Every visit to the page.”

- Images must be auto-loaded.
- Use a high-resolution monitor to maximize the amount of information displayed in the content frame. The recommended resolution is 1024 x 768 pixels. You can also use 800 x 600 pixels.
- Turn off one or more of the browser toolbars to maximize the viewing space of the ExtremeWare Vista content screen.
- If you will be using ExtremeWare Vista to send an email to the Extreme Networks Technical Support department, configure the email settings in your browser.
- Configure the browser to use the following recommended fonts:
  - Proportional font—Times New Roman
  - Fixed-width font—Courier New

## Accessing ExtremeWare Vista

To access the default home page of the switch, enter the following URL in your browser:

`http://<ip_address>`

When you access the home page of the system, you are presented with the Login screen. Enter your user name and password in the appropriate fields, and click OK.

If you have entered the name and password of an administrator-level account, you have access to all ExtremeWare Vista pages. If you have used a user-level account name and password, you only have access to the Statistics and Support information.

If multiple people access the same switch using ExtremeWare Vista, you might see the following error message:

```
Web:server busy
```

To correct this situation, log out of the switch and log in again.

## Navigating ExtremeWare Vista

After logging in to the switch, the ExtremeWare Vista home page is displayed.

ExtremeWare Vista divides the browser screen into the following sections:

- Task frame
- Content frame
- Standalone buttons



## Task Frame

The task frame has two sections: menu buttons and submenu links. The four task menu buttons are:

- Configuration
- Statistics
- Support
- Logout

Below the task buttons are options. Options are specific to the task button that you select. When you select an option, the information displayed in the content frame changes. However, when you select a new task button, the content frame does not change until you select a new option.



### NOTE

---

*Submitting a configuration page with no change will result in an asterisk (\*) appearing at the CLI prompt, even though actual configuration values have not changed.*

## Content Frame

The content frame contains the main body of information in ExtremeWare Vista. For example, if you select an option from the Configuration task button, enter configuration parameters in the content frame. If you select the Statistics task button, statistics are displayed in the content frame.

**Browser Controls.** Browser controls include drop-down list boxes, check boxes, and multiselect list boxes. A multiselect list box has a scrollbar on the right side of the box. Using a multiselect list box, you can select a single item, all items, a set of contiguous items, or multiple noncontiguous items. Table 12 describes how to make selections from a multiselect list box.

**Table 12:** Multiselect List Box Key Definitions

Selection Type	Key Sequence
Single item	Click the item using the mouse.
All items	Click the first item, and drag to the last item.
Contiguous items	Click the first desired item, and drag to the last desired item.
Selected noncontiguous items	Hold down [Ctrl], click the first desired item, click the next desired item, and so on.

## Status Messages

Status messages are displayed at the top of the content frame. The four types of status messages are:

- **Information**—Displays information that is useful to know prior to, or as a result of, changing configuration options.
- **Warning**—Displays warnings about the switch configuration.
- **Error**—Displays errors caused by incorrectly configured settings.
- **Success**—Displays informational messages after you click Submit. The message displayed reads, “Request was submitted successfully.”

## Standalone Buttons

At the bottom of some of the content frames is a section that contains standalone buttons. Standalone buttons are used to perform tasks that are not associated with a particular configuration option. An example of this is the Reboot Switch button.

## Saving Changes

You can save your changes to nonvolatile storage in either of two ways using ExtremeWare Vista:

- Select Save Configuration from the Configuration task button, Switch option.

This field contains a drop-down list box that allows you to select either the primary or secondary configuration area. After you select the configuration area, click Submit to save the changes.

- Click the Logout button.

If you attempt to log out without saving your changes, ExtremeWare Vista prompts you to save your changes.

If you select Yes, the changes are saved to the selected configuration area. To change the selected configuration area, you must go to the Configuration task button, Switch option.

## Filtering Information

Some pages have a Filter button. The Filter button is used to display a subset of information on a given page. For example, on the OSPF configuration page, you can configure authentication based on the VLAN, area identifier, or virtual link. After you select a filtering option and click the Filter button, the form that provides the configuration options displays the available interfaces in the drop-down menu, based on your filtering selection.

Similarly, in certain Configuration and Statistics pages, information is shown based on a particular slot.

Because modular switches allow you to preconfigure modules without having them physically available in the chassis, the configuration pages offer a drop-down menu to select any module card that has been configured on the system, whether or not the module is physically available. By default, information for the first configured module that is found in the chassis is displayed on the page. You can configure available slots and ports by filtering on a selected module from the Sort by Slot drop-down menu.

On the Statistics pages, you can only view information for cards that are configured and physically inserted into the chassis. On these pages, the Sort by Slot drop-down menu displays only these modules.

## Do a GET When Configuring a VLAN

When configuring a VLAN using ExtremeWare Vista, prior to editing the VLAN configuration, you must first click the `get` button to ensure that subsequent edits are applied to the correct VLAN. If you do not click the `get` button and you submit the changes, the changes will be made to the VLAN that was previously displayed.

If you configure a VLAN and then delete it, the *default* VLAN is shown in the VLAN name window, but the VLAN information contained in the lower portion of the page is not updated. Click the `get` button to update the display.

## Sending Screen Output to Extreme Networks

If Extreme Networks requests that you email the output of a particular ExtremeWare Vista screen, follow these steps:

- 1 Click the content frame of the screen that you must send.
- 2 From the Netscape Navigator File menu, select Save Frame As and enter a name for the file.  
From the Microsoft Internet Explorer 3.0 File menu, select Save As and enter a name for the file.  
From Microsoft Internet Explorer 4.0, right-click in the content frame, select View Source, and save the HTML text by copying it and pasting it into a text editor.
- 3 Attach the file to the email message that you are sending to Extreme Networks.

## Using the Simple Network Time Protocol

ExtremeWare supports the client portion of the Simple Network Time Protocol (SNTP) Version 3 based on RFC1769. SNTP can be used by the switch to update and synchronize its internal clock from a Network Time Protocol (NTP) server. When enabled, the switch sends out a periodic query to the indicated NTP server, or the switch listens to broadcast NTP updates. In addition, the switch supports the configured setting for Greenwich Mean time (GMT) offset and the use of Daylight Savings Time. These features have been tested for year 2000 compliance.

## Configuring and Using SNTP

To use SNTP, follow these steps:

- 1 Identify the host(s) that are configured as NTP server(s). Additionally, identify the preferred method for obtaining NTP updates. The options are for the NTP server to send out broadcasts, or for switches using NTP to query the NTP server(s) directly. A combination of both methods is possible. You must identify the method that should be used for the switch being configured.
- 2 Configure the Greenwich Mean Time (GMT) offset and Daylight Savings Time preference. The command syntax to configure GMT offset and usage of Daylight Savings is as follows:

```
config timezone <GMT_offset> {autodst | noautodst}
```

The GMT\_OFFSET is in +/- minutes from the GMT time. Automatic Daylight Savings Time (DST) changes can be enabled or disabled. The default setting is enabled.

- 3 Enable the SNTP client using the following command:

```
enable sntp-client
```

Once enabled, the switch sends out a periodic query to the NTP servers defined later (if configured) or listens to broadcast NTP updates from the network. The network time information is automatically saved into the on-board real-time clock.

- If you would like this switch to use a directed query to the NTP server, configure the switch to use the NTP server(s). If the switch listens to NTP broadcasts, skip this step. To configure the switch to use a directed query, use the following command:

```
config sntp-client [primary | secondary] server [<ip_address> | <hostname>]
```

NTP queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the secondary server (if one is configured). If the switch cannot obtain the time, it restarts the query process. Otherwise, the switch waits for the `sntp-client update interval` before querying again.

- Optionally, the interval for which the SNTP client updates the real-time clock of the switch can be changed using the following command:

```
config sntp-client update-interval <seconds>
```

The default `sntp-client update-interval` value is 64 seconds.

- You can verify the configuration using the following commands:

```
— show sntp-client
```

This command provides configuration and statistics associated with SNTP and its connectivity to the NTP server.

```
— show switch
```

This command indicates the GMT offset, Daylight Savings Time, and the current local time.

NTP updates are distributed using GMT time. To properly display the local time in logs and other timestamp information, the switch should be configured with the appropriate offset to GMT based on geographical location. Table 13 describes GMT offsets.

**Table 13:** Greenwich Mean Time Offsets

GMT Offset in Hours	GMT Offset in Minutes	Common Time Zone References	Cities
+0:00	+0	GMT - Greenwich Mean UT or UTC - Universal (Coordinated) WET - Western European	London, England; Dublin, Ireland; Edinburgh, Scotland; Lisbon, Portugal; Reykjavik, Iceland; Casablanca, Morocco
-1:00	-60	WAT - West Africa	Azores, Cape Verde Islands
-2:00	-120	AT - Azores	
-3:00	-180		Brasilia, Brazil; Buenos Aires, Argentina; Georgetown, Guyana;
-4:00	-240	AST - Atlantic Standard	Caracas; La Paz
-5:00	-300	EST - Eastern Standard	Bogota, Columbia; Lima, Peru; New York, NY, Trevor City, MI USA
-6:00	-360	CST - Central Standard	Mexico City, Mexico
-7:00	-420	MST - Mountain Standard	Saskatchewan, Canada
-8:00	-480	PST - Pacific Standard	Los Angeles, CA, Cupertino, CA, Seattle, WA USA

**Table 13:** Greenwich Mean Time Offsets (continued)

<b>GMT Offset in Hours</b>	<b>GMT Offset in Minutes</b>	<b>Common Time Zone References</b>	<b>Cities</b>
-9:00	-540	YST - Yukon Standard	
-10:00	-600	AHST - Alaska-Hawaii Standard CAT - Central Alaska HST - Hawaii Standard	
-11:00	-660	NT - Nome	
-12:00	-720	IDLW - International Date Line West	
+1:00	+60	CET - Central European FWT - French Winter MET - Middle European MEWT - Middle European Winter SWT - Swedish Winter	Paris, France; Berlin, Germany; Amsterdam, The Netherlands; Brussels, Belgium; Vienna, Austria; Madrid, Spain; Rome, Italy; Bern, Switzerland; Stockholm, Sweden; Oslo, Norway
+2:00	+120	EET - Eastern European, Russia Zone 1	Athens, Greece; Helsinki, Finland; Istanbul, Turkey; Jerusalem, Israel; Harare, Zimbabwe
+3:00	+180	BT - Baghdad, Russia Zone 2	Kuwait; Nairobi, Kenya; Riyadh, Saudi Arabia; Moscow, Russia; Tehran, Iran
+4:00	+240	ZP4 - Russia Zone 3	Abu Dhabi, UAE; Muscat; Tblisi; Volgograd; Kabul
+5:00	+300	ZP5 - Russia Zone 4	
+5:30	+330	IST – India Standard Time	New Delhi, Pune, Allahabad, India
+6:00	+360	ZP6 - Russia Zone 5	
+7:00	+420	WAST - West Australian Standard	
+8:00	+480	CCT - China Coast, Russia Zone 7	
+9:00	+540	JST - Japan Standard, Russia Zone 8	
+10:00	+600	EAST - East Australian Standard GST - Guam Standard Russia Zone 9	
+11:00	+660		
+12:00	+720	IDLE - International Date Line East NZST - New Zealand Standard NZT - New Zealand	Wellington, New Zealand; Fiji, Marshall Islands

## SNTP Configuration Commands

Table 14 describes SNTP configuration commands.

**Table 14:** SNTP Configuration Commands

Command	Description
<code>config sntp-client [primary   secondary] server [&lt;ipaddress&gt;   &lt;host_name&gt;]</code>	Configures an NTP server for the switch to obtain time information. Queries are first sent to the primary server. If the primary server does not respond within 1 second, or if it is not synchronized, the switch queries the second server.
<code>config sntp-client update-interval &lt;seconds&gt;</code>	Configures the interval between polling for time information from SNTP servers. The default setting is 64 seconds.
<code>disable sntp-client</code>	Disables SNTP client functions.
<code>enable sntp-client</code>	Enables Simple Network Time Protocol (SNTP) client functions.
<code>show sntp-client</code>	Displays configuration and statistics for the SNTP client.

## SNTP Example

In this example, the switch queries a specific NTP server and a backup NTP server. The switch is located in Cupertino, CA, and an update occurs every 20 minutes. The commands to configure the switch are as follows:

```
config timezone -480 autodst
config sntp-client update interval 1200
enable sntp-client
config sntp-client primary server 10.0.1.1
config sntp-client secondary server 10.0.1.2
```

# 4

## Configuring Ports on a Switch

---

This chapter describes the following topics:

- Port Numbering on page 55
- Enabling and Disabling Switch Ports on page 55
- Load Sharing on the Switch on page 57
- Switch Port-Mirroring on page 59
- Extreme Discovery Protocol on page 61

### Port Numbering

On a Summit 300-48 switch, the port number is a combination of the slot number and the port number. The nomenclature for the port number is as follows:

```
slot:port
```

You can use wildcard combinations (\*) to specify multiple slot and port combinations. The following wildcard combinations are allowed:

- `slot:*` — Specifies all ports on a particular I/O module.
- `slot:x-slot:y` — Specifies a contiguous series of ports on a particular I/O module.
- `slota:x-slotb:y` — Specifies a contiguous series of ports that begin on one I/O module and end on another I/O module.

### Enabling and Disabling Switch Ports

By default, all ports are enabled. To enable or disable one or more ports, use the following command:

```
[enable | disable] ports <portlist>
```

For example, to disable slot 1, ports 3, 5, and 12 through 15 on a Summit 300-48 switch, use the following command:

```
disable ports 1:3,1:5,1:12-1:15
```

## Configuring Switch Port Speed and Duplex Setting

By default, the switch is configured to use autonegotiation to determine the port speed and duplex setting for each port. You can manually configure the duplex setting and the speed of 10/100 Mbps ports.

10BASE-T and 100BASE-TX ports can connect to either 10BASE-T or 100BASE-T networks. By default, the ports autonegotiate port speed. You can also configure each port for a particular speed (either 10 Mbps or 100 Mbps).

All ports on a stand-alone switch can be configured for half-duplex or full-duplex operation. By default, the 10/100 Mbps ports autonegotiate the duplex setting.

To configure port speed and duplex setting, use the following command:

```
config ports <portlist> auto off speed [10 | 100 | 1000] duplex [half | full]
```

To configure the system to autonegotiate, use the following command:

```
config ports <portlist> auto on
```

## Switch Port Commands

Table 15 describes the switch port commands.

**Table 15:** Switch Port Commands

Command	Description
config ports <portlist> auto off speed [10   100   1000] duplex [half   full]	Changes the configuration of a group of ports. Specify the following: <ul style="list-style-type: none"> <li>• <code>auto off</code> — The port will not autonegotiate the settings.</li> <li>• <code>speed</code> — The speed of the port.</li> <li>• <code>duplex</code> — The duplex setting (half- or full-duplex).</li> </ul>
config ports <portlist> auto on	Enables autonegotiation for the particular port type; 802.3u for 10/100 Mbps ports or 802.3z for Gigabit Ethernet ports.
config ports <portlist> display-string <string>	Configures a user-defined string for a port. The string is displayed in certain <code>show</code> commands (for example, <code>show ports info</code> ). The string can be up to 16 characters.
config sharing address-based [mac_source   mac_destination   mac_source_destination   ip_source   ip_destination   ip_source_destination]	Configures the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is available using the address-based load-sharing algorithm, only.
disable ports <portlist>	Disables a port. Even when disabled, the link is available for diagnostic purposes.
disable sharing <port>	Disables a load-sharing group of ports.
enable ports <portlist>	Enables a port.



**Table 15:** Switch Port Commands (continued)

Command	Description
enable sharing <port> grouping <portlist> {address-based}	Defines a load-sharing group of ports. The ports specified in <portlist> are grouped to the master port. The optional load-sharing algorithm, address-based, uses addressing information as criteria for egress port selection.
restart ports <portlist>	Resets autonegotiation for one or more ports by resetting the physical link.
show ports {<portlist>} collisions	Displays real-time collision statistics.
show ports {<portlist>} configuration	Displays the port configuration.
show ports {<portlist>} info {detail}	Displays detailed system-related information.
show ports {<portlist>} packet	Displays a histogram of packet statistics.
show ports {<portlist>} rxerrors	Displays real-time receive error statistics.
show ports {<portlist>} stats	Displays real-time port statistics.
show ports {<portlist>} txerrors	Displays real-time transmit error statistics.
show ports {<portlist>} utilization	Displays real-time port utilization information. Use the [Spacebar] to toggle between packet, byte, and bandwidth utilization information.
show sharing address-based	Displays the address-based load sharing configuration.
unconfig ports <portlist> display-string <string>	Clears the user-defined display string from a port.

## Load Sharing on the Switch

Load sharing with switches allows you to increase bandwidth and resiliency by using a group of ports to carry traffic in parallel between switches. The sharing algorithm allows the switch to use multiple ports as a single logical port. For example, VLANs see the load-sharing group as a single logical port. Most load-sharing algorithms guarantee packet sequencing between clients.

If a port in a load-sharing group fails, traffic is redistributed to the remaining ports in the load-sharing group. If the failed port becomes active again, traffic is redistributed to include that port.

This feature is supported between Extreme Networks switches only, but may be compatible with third-party trunking or link-aggregation algorithms. Check with an Extreme Networks technical representative for more information.



### NOTE

*Load sharing must be enabled on both ends of the link or a network loop may result. The load-sharing algorithms do not need to be the same on both ends.*

## Load-Sharing Algorithms

Load-sharing algorithms allow you to select the distribution technique used by the load-sharing group to determine the output port selection. Algorithm selection is not intended for use in predictive traffic engineering.

You can configure the address-based load-sharing algorithm on the Summit 300-48 switch.

The address-based load-sharing algorithm uses addressing information to determine which physical port in the load-sharing group to use for forwarding traffic out of the switch. Addressing information is based on the packet protocol, as follows:

- IP packets — Uses the source and destination MAC and IP addresses.
- All other packets — Uses the source and destination MAC address.

## Configured IP Address-Based Load Sharing

When you configure load sharing, the switch examines a specific place in the packet to determine which egress port to use for forwarding traffic:

- For Layer 2 load sharing, the switch uses the MAC source address, MAC destination address, IP source address, and IP destination address.
- For Layer 3 load sharing, the switch uses the IP destination address.

You can control the field examined by the switch for IP address-based load sharing, using the following command:

```
config sharing address-based [mac_source | mac_destination | mac_source_destination |
ip_source | ip_destination | ip_source_destination]
```

where:

- `mac_source` — Indicates that the switch should examine the MAC source address.
- `mac_destination` — Indicates that the switch should examine the MAC destination address.
- `mac_source_destination` — Indicates that the switch should examine the MAC source and destination address.
- `ip_source` — Indicates that the switch should examine the IP source address.
- `ip_source_destination` — Indicates that the switch should examine the IP source address and destination address.
- `ip_destination` — Indicates that the switch should examine the IP destination address.

This feature is available for the address-based load-sharing algorithm, only.

To verify your configuration, use the following command:

```
show sharing address-based
```

## Configuring Switch Load Sharing

To set up a switch to load share among ports, you must create a load-sharing group of ports. The first port in the load-sharing group is configured to be the “master” logical port. This is the reference port used in configuration commands. It can be thought of as the logical port representing the entire port group.

The following rules apply to the Summit 300-48 switch:

- Ports on the switch must be of the same port type. For example, if you use 100 Mbps ports, all ports on the switch must be 100 Mbps ports.

- Ports on the switch are divided into a maximum of five groups.
- Port-based and round-robin load sharing algorithms do not apply.
- A redundant load share group can only include ports from the following ranges: 1:1-1:24, 1:25-1:48, 1:49-1:52.

To define a load-sharing group, you assign a group of ports to a single, logical port number. To enable or disable a load-sharing group, use the following commands:

```
enable sharing <port> grouping <portlist> {address-based}
disable sharing <port>
```



*A maximum of eight ports in a load-share group is allowed.*

## Load-Sharing Example

This section provides an example of how to define load-sharing on a Summit 300-48 switch.

### Load-Sharing on a Summit 300-48 Switch

The following example defines a load-sharing group that contains ports 1:9 through 1:12, and uses the first port in the group as the master logical port 9:

```
enable sharing 1:9 grouping 1:9-1:12
```

In this example, logical port 9 represents physical ports 1:9 through 1:12.

When using load sharing, you should always reference the master logical port of the load-sharing group (port 1:9 in the previous example) when configuring or viewing VLANs. VLANs configured to use other ports in the load-sharing group will have those ports deleted from the VLAN when load sharing becomes enabled.

## Verifying the Load-Sharing Configuration

The screen output resulting from the `show ports configuration` command lists the ports that are involved in load sharing and the master logical port identity.

## Switch Port-Mirroring

Port-mirroring configures the switch to copy all traffic associated with one or more ports. The monitor port can be connected to a network analyzer or RMON probe for packet analysis. The system uses a traffic filter that copies a group of traffic to the monitor port.

The traffic filter is defined by the following criteria:

- **Physical port** — All data that traverses the port, regardless of VLAN configuration, is copied to the monitor port.

Up to eight mirroring filters and one monitor port can be configured. After a port has been specified as a monitor port, it cannot be used for any other function.

**NOTE**


---

*Frames that contain errors are not mirrored.*

The mirrored port always transmits tagged frames. The default port tag will be added to any untagged packets as they are mirrored. This allows you to mirror multiple ports or VLANs to a mirror port, while preserving the ability of a single protocol analyzer to track and differentiate traffic within a broadcast domain (VLAN) and across broadcast domains (for example, across VLANs when routing).

**NOTE**


---

*For optimum performance, mirror three or fewer ports at any given time.*

- Mirror ports and monitor ports should both be confined to the following ranges: 1:1-1:24, 1:25-1:48, 1:49-1:52.

## Port-Mirroring Commands

Switch port-mirroring commands are described in Table 16.

**Table 16:** Switch Port-Mirroring Configuration Commands

Command	Description
config mirroring add ports <portlist>	Adds a single mirroring filter definition. Up to eight mirroring definitions can be added.
config mirroring delete ports <portlist>	Deletes a particular mirroring filter definition.
disable mirroring	Disables port-mirroring.
enable mirroring to <port> tagged	Dedicates a port to be the mirror output port. Port must be active before enabling mirroring.
show mirroring	Displays the port-mirroring configuration.

## Port-Mirroring Example

The following example selects port 1:3 as the mirror port and sends all traffic coming into or out of the switch on port 1:1 to the mirror port:

```
enable mirroring to port 1:3 tagged
config mirroring add port 1:1
```

## Extreme Discovery Protocol

The Extreme Discovery Protocol (EDP) is used to gather information about neighbor Extreme Networks switches. EDP is used by the switches to exchange topology information. Information communicated using EDP includes:

- Switch MAC address (switch ID).
- Switch software version information.
- Switch IP address.
- Switch VLAN-IP information.
- Switch port number.



### CAUTION

*With EDP enabled, none of the wireless ports will be able to participate in the AccessAdapt protocol which is based on EDP. For more information about wireless ports, see Chapter 6.*

## EDP Commands

Table 17 lists EDP commands.

**Table 17:** EDP Commands

Command	Description
disable edp ports <portlist>	Disables the EDP on one or more ports.
enable edp ports <portlist>	Enables the generation and processing of EDP messages on one or more ports. The default setting is enabled.
show edp	Displays EDP information.



# 5

## Virtual LANs (VLANs)

---

This chapter describes the following topics:

- Overview of Virtual LANs on page 63
- Types of VLANs on page 64
- VLAN Names on page 69
- Configuring VLANs on the Switch on page 70
- Displaying VLAN Settings on page 71

Setting up Virtual Local Area Networks (VLANs) on the switch eases many time-consuming tasks of network administration while increasing efficiency in network operations.

### Overview of Virtual LANs

The term VLAN is used to refer to a collection of devices that communicate as if they were on the same physical LAN. Any set of ports (including all ports on the switch) is considered a VLAN. LAN segments are not restricted by the hardware that physically connects them. The segments are defined by flexible user groups you create with the command-line interface.

### Benefits

Implementing VLANs on your networks has the following advantages:

- **VLANs help to control traffic.**

With traditional networks, congestion can be caused by broadcast traffic that is directed to all network devices, regardless of whether they require it. VLANs increase the efficiency of your network because each VLAN can be set up to contain only those devices that must communicate with each other.

- **VLANs provide extra security.**

Devices within each VLAN can only communicate with member devices in the same VLAN. If a device in VLAN *Marketing* must communicate with devices in VLAN *Sales*, the traffic must cross a routing device.

- **VLANs ease the change and movement of devices.**

With traditional networks, network administrators spend much of their time dealing with moves and changes. If users move to a different subnetwork, the addresses of each endstation must be updated manually.

## Types of VLANs

VLANs can be created according to the following criteria:

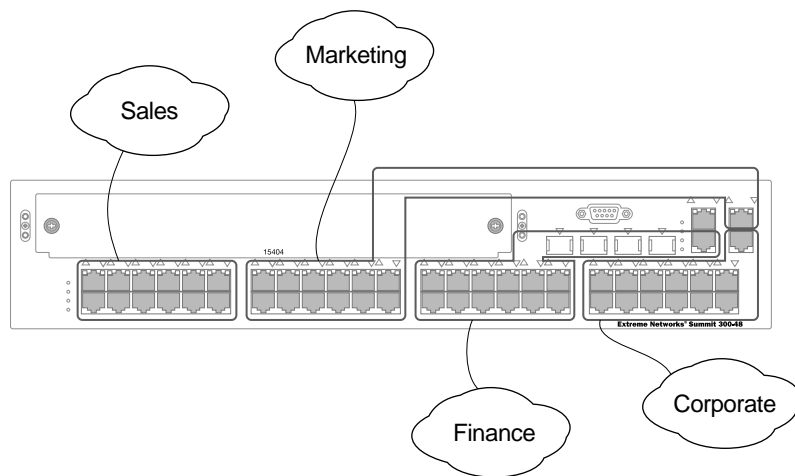
- Physical port
- 802.1Q tag
- A combination of these criteria

### Port-Based VLANs

In a port-based VLAN, a VLAN name is given to a group of one or more ports on the switch. A port can be a member of only one port-based VLAN. The Summit 300-48 switch supports L2 port-based VLANs.

For example, on the Summit 300-48 switch in Figure 1, ports 1:1 through 1:12 are part of VLAN *Sales*; ports 1:13 through 1:24, and port 1:51 are part of VLAN *Marketing*; ports 1:25 through 1:36, and port 1:50 are part of VLAN *Finance*, and ports 1:37 through 1:48, and port 1:52 are part of VLAN *Corporate*.

**Figure 1:** Example of a port-based VLAN on the Summit 300-48 switch



LB48005

For the members of the different IP VLANs to communicate, the traffic must be routed by the switch. This means that each VLAN must be configured as a router interface with a unique IP address.



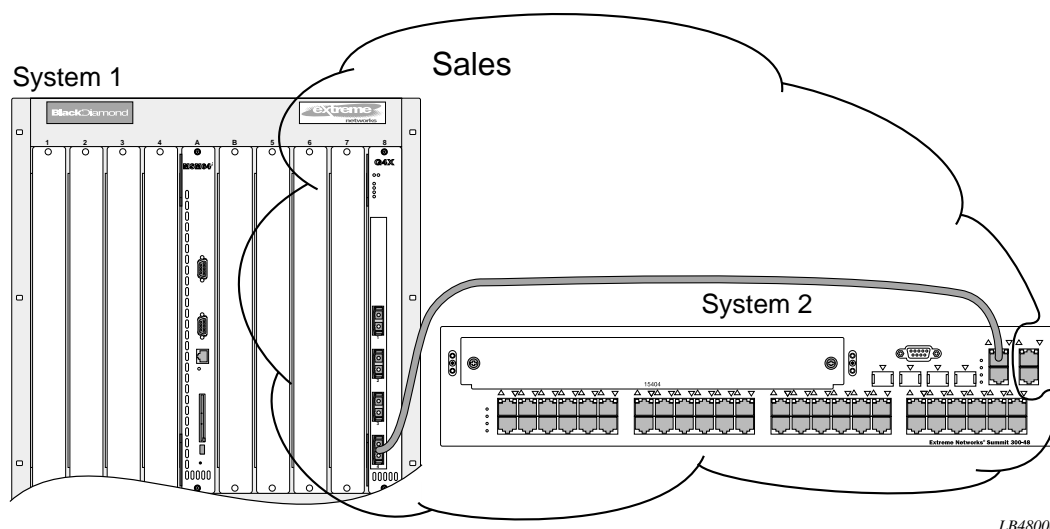
## Spanning Switches with Port-Based VLANs

To create a port-based VLAN that spans two switches, you must do two things:

- 1 Assign the port on each switch to the VLAN.
- 2 Cable the two switches together using one port on each switch per VLAN.

Figure 2 illustrates a single VLAN that spans a BlackDiamond switch and a Summit 300-48 switch. All ports on the BlackDiamond switch belong to VLAN *Sales*. Ports 1:1 through 1:24, and port 1:26 on the Summit 300-48 switch also belong to VLAN *Sales*. The two switches are connected using slot 8, port 4 on system 1 (the BlackDiamond switch), and port 1:26 on system 2 (the Summit 300-48 switch).

**Figure 2:** Single port-based VLAN spanning two switches

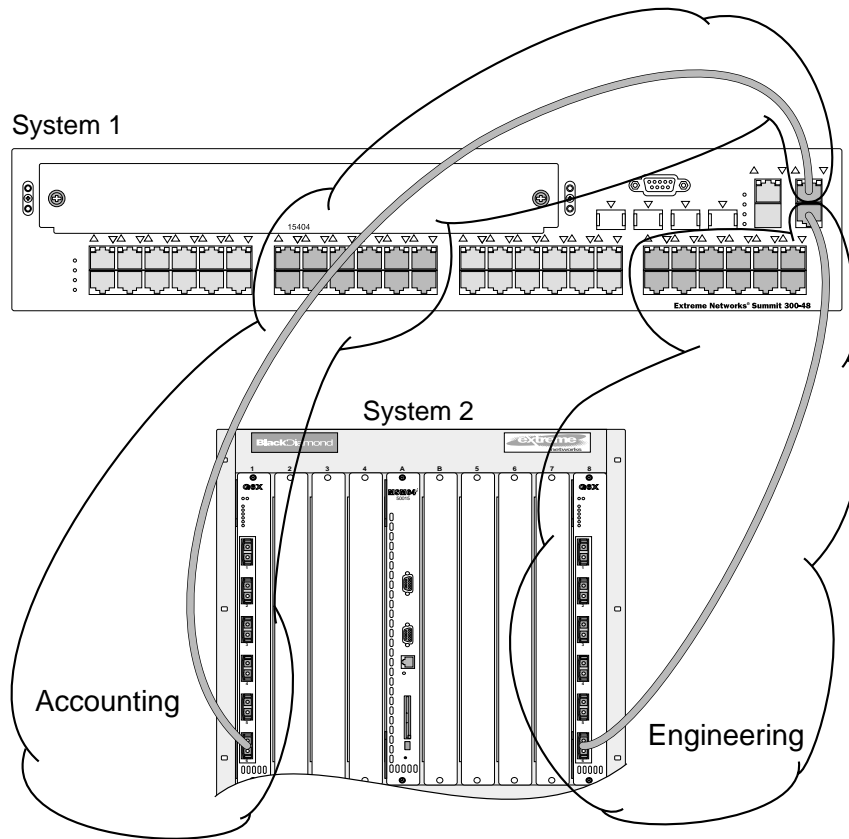


LB48006

To create multiple VLANs that span two switches in a port-based VLAN, a port on system 1 must be cabled to a port on system 2 for each VLAN you want to have span across the switches. At least one port on each switch must be a member of the corresponding VLANs, as well.

Figure 3 illustrates two VLANs spanning two switches. On system 1, ports 1:12 through 1:24, and port 1:51 are part of VLAN *Accounting*; ports 1:37 through 1:48, and port 1:52 are part of VLAN *Engineering*. On system 2, all ports on slot 1 are part of VLAN *Accounting*; all ports on slot 8 are part of VLAN *Engineering*.

**Figure 3:** Two port-based VLANs spanning two switches



LB48007

VLAN *Accounting* spans system 1 and system 2 by way of a connection between system 1, port 1:51 and system 2, slot 1, port 6. VLAN *Engineering* spans system 1 and system 2 by way of a connection between system 1, port 1:52, and system 2, slot 8, port 6.

Using this configuration, you can create multiple VLANs that span multiple switches, in a daisy-chained fashion. Each switch must have a dedicated port for each VLAN. Each dedicated port must be connected to a port that is a member of its VLAN on the next switch.

## Tagged VLANs

*Tagging* is a process that inserts a marker (called a *tag*) into the Ethernet frame. The tag contains the identification number of a specific VLAN, called the *VLANid*. The Summit 300-48 switch supports L2 tagged VLANs.

**NOTE**

*The use of 802.1Q tagged packets may lead to the appearance of packets slightly bigger than the current IEEE 802.3/Ethernet maximum of 1,518 bytes. This may affect packet error counters in other devices, and may also lead to connectivity problems if non-802.1Q bridges or routers are placed in the path. The tag also carries the 802.1 (802.1p) priority bits. This is the only way priority information can be shared between separate devices (hosts, switches/routers and so on).*

**Uses of Tagged VLANs**

Tagging is most commonly used to create VLANs that span switches. The switch-to-switch connections are typically called *trunks*. Using tags, multiple VLANs can span multiple switches using one or more trunks. In a port-based VLAN, each VLAN requires its own pair of trunk ports, as shown in Figure 3. Using tags, multiple VLANs can span two switches with a single trunk.

Another benefit of tagged VLANs is the ability to have a port be a member of multiple VLANs. This is particularly useful if you have a device (such as a server) that must belong to multiple VLANs. The device must have a NIC that supports 802.1Q tagging.

A single port can be a member of only one port-based VLAN. All additional VLAN membership for the port must be accompanied by tags. In addition to configuring the VLAN tag for the port, the server must have a *Network Interface Card (NIC)* that supports 802.1Q tagging.

**Assigning a VLAN Tag**

Each VLAN may be assigned an 802.1Q VLAN tag. As ports are added to a VLAN with an 802.1Q tag defined, you decide whether each port will use tagging for that VLAN. The default mode of the switch is to have all ports assigned to the VLAN named *default* with an 802.1Q VLAN tag (VLANid) of 1 assigned.

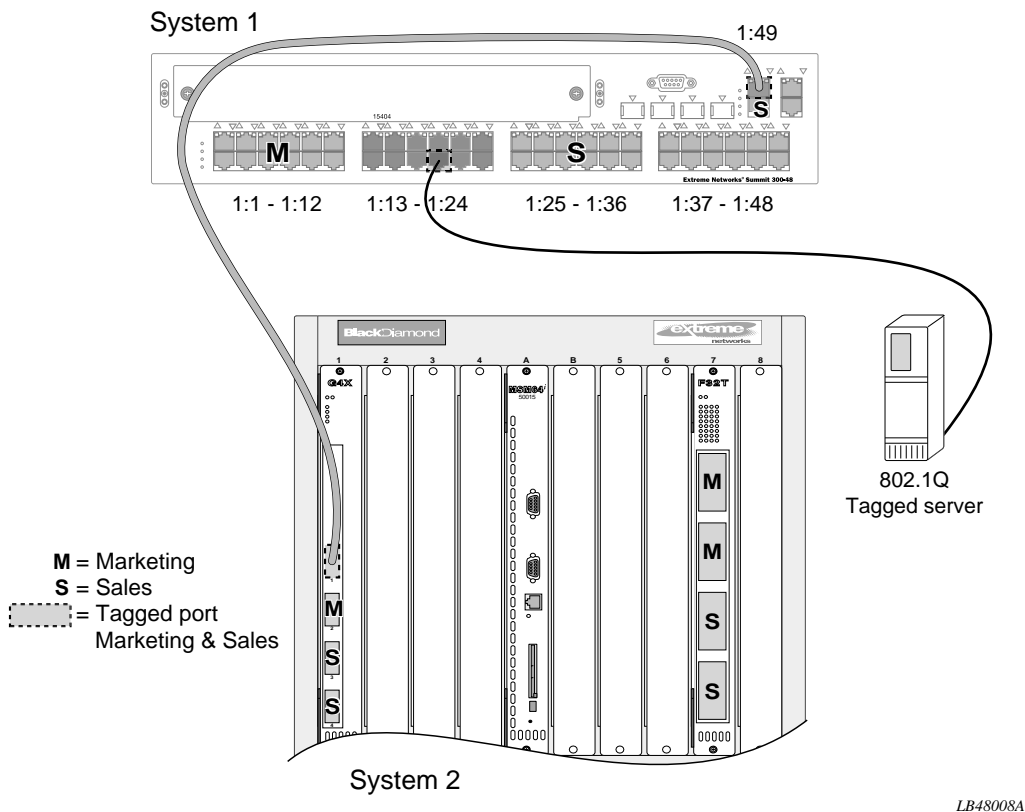
Not all ports in the VLAN must be tagged. As traffic from a port is forwarded out of the switch, the switch determines (in real time) if each destination port should use tagged or untagged packet formats for that VLAN. The switch adds and strips tags, as required, by the port configuration for that VLAN.

**NOTE**

*Packets arriving tagged with a VLANid that is not configured on a port will be discarded.*

Figure 4 illustrates the physical view of a network that uses tagged and untagged traffic.

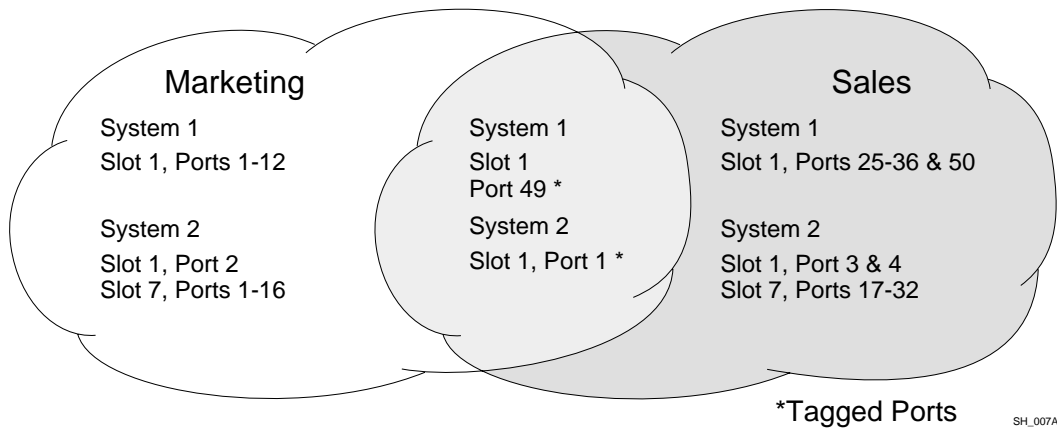
**Figure 4:** Physical diagram of tagged and untagged traffic



LB48008A

Figure 5 is a logical diagram of the same network.

**Figure 5:** Logical diagram of tagged and untagged traffic



SH\_007A

In Figure 4 and Figure 5:

- The trunk port on each switch carries traffic for both VLAN *Marketing* and VLAN *Sales*.
- The trunk port on each switch is tagged.

- The server connected to port 1:16 on system 1 has a NIC that supports 802.1Q tagging.
- The server connected to port 1:16 on system 1 is a member of both VLAN *Marketing* and VLAN *Sales*.
- All other stations use untagged traffic.

As data passes out of the switch, the switch determines if the destination port requires the frames to be tagged or untagged. All traffic coming from and going to the server is tagged. Traffic coming from and going to the trunk ports is tagged. The traffic that comes from and goes to the other stations on this network is not tagged.

### Mixing Port-Based and Tagged VLANs

You can configure the switch using a combination of port-based and tagged VLANs. A given port can be a member of multiple VLANs, with the stipulation that only one of its VLANs uses untagged traffic. In other words, a port can simultaneously be a member of one port-based VLAN and multiple tag-based VLANs.



#### NOTE

---

*For the purposes of VLAN classification, packets arriving on a port with an 802.1Q tag containing a VLANid of zero are treated as untagged.*

## VLAN Names

Each VLAN is given a name that can be up to 32 characters. VLAN names can use standard alphanumeric characters. The following characters are not permitted in a VLAN name:

- Space
- Comma
- Quotation mark

VLAN names must begin with an alphabetical letter. Quotation marks can be used to enclose a VLAN name that does not begin with an alphabetical character, or that contains a space, comma, or other special character.

VLAN names are locally significant. That is, VLAN names used on one switch are only meaningful to that switch. If another switch is connected to it, the VLAN names have no significance to the other switch.



#### NOTE

---

*You should use VLAN names consistently across your entire network.*

### Default VLAN

The switch ships with one default VLAN that has the following properties:

- The VLAN name is *default*.
- It contains all the ports on a new or initialized switch.
- The default VLAN is untagged on all ports. It has an internal VLANid of 1.

## Renaming a VLAN

To rename an existing VLAN, use the following command:

```
config vlan <old_name> name <new_name>
```

The following rules apply to renaming VLANs:

- After you change the name of the default VLAN, it cannot be changed back to *default*.
- You cannot create a new VLAN named *default*.

## Configuring VLANs on the Switch

This section describes the commands associated with setting up VLANs on the switch. Configuring a VLAN involves the following steps:

- 1 Create and name the VLAN.
- 2 Assign an IP address and mask (if applicable) to the VLAN, if needed.



### NOTE

Each IP address and mask assigned to a VLAN must represent a unique IP subnet. You cannot configure the same IP subnet on different VLANs.

- 3 Assign a VLANid, if any ports in this VLAN will use a tag.
- 4 Assign one or more ports to the VLAN.  
As you add each port to the VLAN, decide if the port will use an 802.1Q tag.

## VLAN Configuration Commands

Table 18 describes the commands used to configure a VLAN.

**Table 18:** VLAN Configuration Commands

Command	Description
config vlan <name> add port <portlist> {tagged   untagged} {nobroadcast}	Adds one or more ports to a VLAN. You can specify tagged port(s), untagged port(s). Specify <i>nobroadcast</i> to prevent the switch from forwarding broadcast, multicast, and unknown unicast traffic. By default, ports are untagged.
config vlan <name> delete port <portlist> {tagged   untagged} {nobroadcast}	Deletes one or more ports from a VLAN.
config vlan <name> ipaddress <ipaddress> {<mask>}	Assigns an IP address and an optional mask to the VLAN.
config vlan <name> tag <vlanid>	Assigns a numerical VLANid. The valid range is from 2 to 4094 (1 is used by the default VLAN).
config vlan <old_name> name <new_name>	Renames a previously configured VLAN.
create vlan <name>	Creates a named VLAN.

**Table 18:** VLAN Configuration Commands (continued)

Command	Description
delete vlan <name>	Removes a VLAN.
unconfig ports <portlist> monitor vlan <name>	Removes port-based VLAN monitoring.
unconfig vlan <name> ipaddress	Resets the IP address of the VLAN.

## VLAN Configuration Examples

The following Summit 300-48 switch example creates a tag-based VLAN named *video*. It assigns the VLANid 1000. Ports 1:4 through 1:8 are added as tagged ports to the VLAN.

```
create vlan video
config video tag 1000
config video add port 1:4-1:8 tagged
```

The following Summit 300-48 switch example creates a VLAN named *sales*, with the VLANid 120. The VLAN uses both tagged and untagged ports. Ports 1:1 through 1:3 are tagged, and ports 1:4 and 1:7 are untagged. Note that when not explicitly specified, ports are added as untagged.

```
create vlan sales
config sales tag 120
config sales add port 1:1-1:3 tagged
config sales add port 1:4,1:7
```

## Displaying VLAN Settings

To display VLAN settings, use the following command:

```
show vlan {<name>} {detail}
```

The `show` command displays summary information about each VLAN, which includes:

- Name
- VLANid
- How the VLAN was created
- IP address
- STPD information
- QoS profile information
- Ports assigned
- Tagged/untagged status for each port
- How the ports were added to the VLAN
- Number of VLANs configured on the switch

Use the `detail` option to display the detailed format.





# 6

## Wireless Networking

---

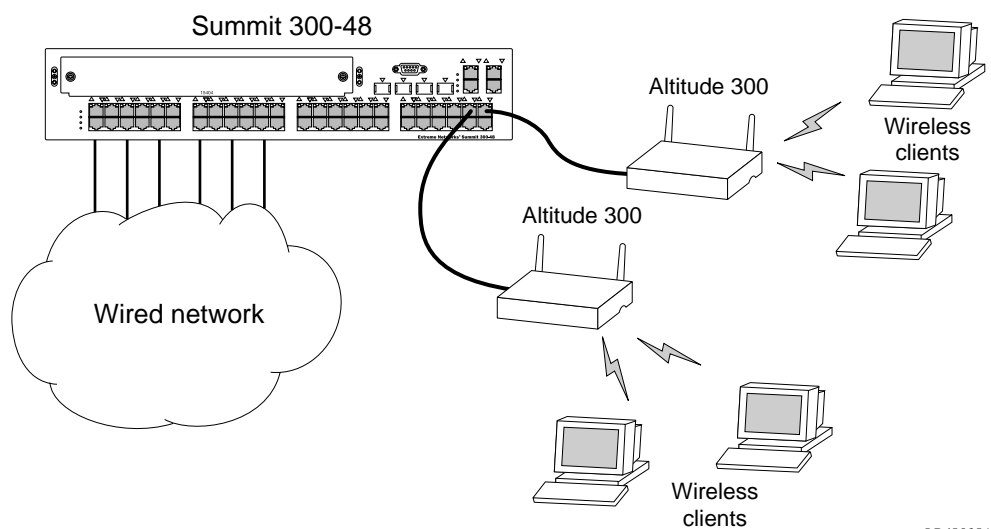
This chapter describes wireless networking using the Summit 300-48 switch and the Altitude 300 wireless port and includes information on the following topics:

- Overview of Wireless Networking on page 73
- Wireless Devices on page 74
- Bridging on page 75
- Configuring RF Properties on page 76
- Configuring Wireless Switch Properties on page 78
- Configuring Wireless Ports on page 79
- Configuring Wireless Port Interfaces on page 79
- Managing Wireless Clients on page 80
- Show Commands on page 80
- Event Logging and Reporting on page 81

### Overview of Wireless Networking

The Summit 300-48 switch and the Altitude 300 wireless port extend network service to wireless 802.11a/b/g clients within a fully integrated network infrastructure. Ports on the Summit 300-48 switch handle all of the management functions typically associated with an access point. The Altitude 300 wireless port serves as the radio transmitter and receiver, inheriting configuration information as soon as it is attached to the switch and as changes are made to the wireless profiles after the system is deployed.

Figure 6 shows a sample network configuration. The Summit 300-48 switch provides switching service across the wired and wireless network. Each port on the switch is configured with a “personality” that identifies its function.

**Figure 6:** Sample integrated wired and wireless network

LB48018A

This arrangement is part of the Extreme Unified Access Architecture, which is designed to support both wired and wireless networks from a single network switch. Because the intelligence normally associated with an access point is maintained in the Summit 300-48 switch, the cost of implementing radio access is greatly reduced. The network can still be expanded as needed, but it becomes much easier to maintain security and reliability at reduced cost.

## Summary of Wireless Features

The Summit 300-48 switch supports the following wireless features:

- Simultaneous support for 802.11a, 802.11b, and 802.11g
- EAP authentication for 802.1X devices—PEAP, EAP-TLS, and EAP-TTLS
- WPA using TKIP and AES
- Per-user VLAN classification
- AccessAdapt™ management
- Remote troubleshooting
- Easy upgrading of wireless ports
- Detailed reports and logging

## Wireless Devices

You configure ports on the Summit 300-48 switch with the “personality” of the device to be connected. Each port contains separately configurable interfaces for each of its two radios (A and G).

Physical security for the wireless networks ceases to be a problem at the wireless access location, since the Altitude 300 wireless port does not store any security settings. Information is not stored in the Altitude 300 wireless port, but loaded as needed from the switch. Even if the Altitude 300 wireless port is physically moved, it can only be reconnected to another Summit 300-48 switch.

You can set network policies at Layers 2 and 3 to cover both the wired and wireless networks. In this way you can block access to individuals suspected of intrusion across the entire network infrastructure.

In addition to traditional wired devices, the Summit 300-48 switch supports the Altitude 300 wireless port, third party access points, and devices that rely on Power over Ethernet (PoE).

## Bridging

The bridging module provides support for wireless-to-wireless and wireless-to-Ethernet bridging, including the following features:

- Multiple transmit queues for the wireless interface
- User identity-based VLANs, in which each station is associated with a VLAN based on authentication results
- 802.1p with priority level based on the ToS/DiffServ bit in the IP header

## Managing Wireless Ports

It is not necessary to configure the individual Altitude 300 wireless ports. You set port attributes on the Summit 300-48 switch, copying them as needed to new ports that you configure. Each time you make a change to wireless configuration on the switch, that change is implemented in the wireless network. Upgrading wireless software becomes extremely easy, since it is only necessary to upgrade the switch, not the wireless ports.

There are two interfaces (A and G) available on each Summit 300-48 switch port. All CLI commands refer to the A radio as interface 1 and the G radio as interface 2.

Device management is flexible. From the management system you can enable and disable individual wireless ports or sets of ports based on time, user, or location. You manage the wireless ports from the wired IP network.

Profiles are available for security and RF parameters. Profiles function as templates, eliminating the need to issue repetitive commands and thereby simplifying the process of updating configuration information over multiple ports. You assign profiles to each interface (A or G) on a port and share the profiles across ports. Unless otherwise specified, a default profile is automatically assigned to each new wireless port.

Follow this process to configure wireless ports on the Summit 300-48 switch:

- 1** Designate a VLAN as the wireless management VLAN. Make sure that the VLAN port is untagged between the switch and the Altitude 300 wireless port.
- 2** Assign IP addresses on this VLAN for each wireless port.
- 3** Create RF-profiles.
- 4** Assign an ess-name to the network.
- 5** Create security profiles and configure security parameters for each.
- 6** Configure wireless ports on the switch by assigning RF profiles and security profiles.

- 7 Configure a specific channel (determined from a site survey), if desired, on each interface. If you do not configure a specific channel, the switch auto-selects the channel with the least interference.
- 8 Connect the Altitude 300 wireless port.

After this process is complete, clients can access your network through the Altitude 300 wireless port.

## Configuring RF Properties

RF profiles allow you to group RF parameters for access using a single CLI command. The following rules apply for RF profiles:

- After you have defined a profile, subsequent changes automatically apply to all ports assigned to that profile.
- Each RF profile applies to a specific interface (A or G), so changing a profile only affects the specified interface.
- Each RF profile applies only to ports that support the same version of the Altitude 300 wireless port, thereby preventing problems with version/capability mismatches.
- Each Summit 300-48 switch ships with default profiles for each supported wireless port.

**Table 19:** RF Configuration Commands

Command	Description
create rf-profile <name> copy <name>	Creates a new profile identified by the string name. The copy argument specifies the name of an existing profile from which to obtain the initial values.
create rf-profile <name> mode [A   G]	Creates a new profile identified by the string name. The mode argument specifies the interface mode A or G.
delete rf-profile <name>	Deletes the named RF profile. The named profile cannot be attached to any active ports.
config rf-profile <name> <property> <value>	Sets the value of the property in the named profile to the specified value. Changes take effect immediately and are propagated to all ports that share this profile. All failures are written to the syslog. See Table 20 for <property> values.

**Table 20:** RF Profile Property Values

Property	Default	Allowed Values	Description
ess-name	default_ESS	1-32 characters	Identified as a character string. Default values are per-channel (A   G); string names reflect this.
beacon-interval	40	20-1000	Indicates the frequency interval of the beacon in milliseconds. A beacon is a packet broadcasted by the wireless port to synchronize the wireless network.

**Table 20:** RF Profile Property Values (continued)

Property	Default	Allowed Values	Description
frag-length	2345	256-2345	Identifies fragment size in bytes. This value should remain at its default setting of 2345. It specifies the maximum size for a packet before data is fragmented into multiple packets. If you experience a high packet error rate, you may slightly increase the fragmentation threshold. Setting the fragmentation threshold too low may result in poor network performance. Only minor modifications of this value are recommended.
dtim-interval	2	1-100	Indicates the interval of the delivery traffic indication message (DTIM) in milliseconds. A DTIM field is a countdown field informing clients of the next window for listening to broadcast and multicast messages. When the wireless port has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value. Its clients hear the beacons and awaken to receive the broadcast and multicast messages.
rts-threshold	2330	0-2347	Identifies request to send (RTS) threshold in bytes. Should you encounter inconsistent data flow, only minor modifications are recommended. If a network packet is smaller than the preset RTS threshold size, the RTS and clear to send (CTS) mechanism is not enabled. The wireless port sends RTS frames to a particular receiving station and negotiates the sending of a data frame. After receiving an RTS, the wireless station responds with a CTS frame to acknowledge the right to begin transmission.
preamble	short	short   long	Gives the size of the packet preamble
max-clients	64	1-128	Specifies the maximum number of clients allowed to connect simultaneously.
short-retry	4	1-255	Indicates the number of transmission attempts of a frame, the length of which is less than or equal to <code>rts-threshold</code> , made before a failure condition is indicated.
long-retry	7	1-255	Indicates the number of transmission attempts of a frame, the length of which is greater than <code>rts-threshold</code> , made before a failure condition is indicated.

## Configuring Wireless Switch Properties

Table 21 lists the wireless configuration command that applies to the switch as a whole, independent of individual ports or port interfaces. Table 22 lists the command properties.

**Table 21:** Switch-Level Wireless Configuration Commands

Command	Description
configure wireless <property>	Configures properties that are independent of the port or port interface. See Table 22 for <property> values.

**Table 22:** Switch-Level Configuration Property Values

Property	Default	Allowed Values	Description
country-code	extreme_default	Refer to Release Notes.	Sets the country identifier for the switch.
default-gateway	NA	NA	Indicates the IP address of the default gateway. By default, this is the same IP address as the management VLAN.
management-vlan	default	NA	Identifies the VLAN on which the Altitude 300 wireless port communicates with the Summit 300-48 switch.

## Configuring Country Codes

When the Summit 300-48 switch is set to factory defaults, you must configure the correct country code using the country code properties listed in Table 22.

Extreme Networks ships the Summit 300-48 switch to be programmed with Extreme Network's special `extreme_default` country code, which brings up only the G radio in channel 6, and turns off the A radio. When an Altitude 300 wireless port is connected and the Summit 300-48 switch is unable to determine the country for which the Altitude is programmed, then the `extreme_default` country code is used. You must program the country code on the Summit 300-48 switch to enable the remaining channels for the desired country.

The Altitude 300 wireless port is shipped with a pre-programmed code for certain countries where required by law, and as 'Rest of World' for other countries. If you do not program the country code in the Summit 300-48 switch, then the switch inherits the country code of the first Altitude 300 wireless port that connects to it, if the Altitude is not programmed for the 'Rest of World'.

If there is a mismatch between the country codes between the Altitude 300 wireless port and the code programmed on the Summit 300-48 switch, then the Altitude 300 wireless port is not allowed to come up.

## Configuring Wireless Ports

The `configure wireless ports` commands allow you to configure properties such as the IP address and the location of the port.

Table 23 lists the configuration commands for wireless ports.

**Table 23:** Wireless Port Configuration Commands

Command	Description
<code>config wireless ports &lt;portlist&gt; &lt;property&gt;</code>	Configures the named property for the specified port or ports. See Table 24 for <property> values.
<code>reset wireless ports &lt;portlist&gt;</code>	Resets the specified ports.
<code>enable   disable wireless ports &lt;portlist&gt;</code>	Administratively enables or disables a wireless port for use.
<code>enable   disable wireless ports &lt;portlist&gt; time &lt;date&gt; &lt;hour&gt;</code>	Enables   Disables the specified ports at the given date (m/d/yyyy) and hour (0-23).
<code>enable   disable wireless ports &lt;portlist&gt; every &lt;hour&gt;</code>	Enables   Disables the specified ports every date at the specified hour.
<code>enable   disable wireless ports &lt;portlist&gt; cancel-scheduler</code>	Cancels previously scheduled enable or disable scheduling commands for the port.

Table 24 identifies property values for the `wireless port` configuration commands.

**Table 24:** Wireless Port Configuration Property Values

Property	Default	Allowed Values	Description
<code>ipaddress</code>	192.168.0.100 + port number (1-48)	NA	Indicates the source IP address. The IP address must be an IP address on the management VLAN.
<code>location</code>	"Unknown Location"	N/A	Identifies the location to be configured.
<code>health-check</code>	on	off   on	Indicates whether the health check reset function is on or off. This determines whether the port should be reset if the health check timer expires.

## Configuring Wireless Port Interfaces

Each wireless port on the Summit 300-48 switch contains two interfaces. Interface 1 supports 802.11A, and interface 2 supports 802.11G radio signals. The `configure wireless port interface` commands allow you to configure one of the two individual interfaces (1 | 2) on a port or ports. You can move an interface from one profile to another without having to shut it down.

Table 25 lists the configuration commands for wireless ports.

**Table 25:** Wireless Port Interface Configuration Commands

Command	Description
config wireless ports <portlist> interface [1   2] rf-profile <name>	Attaches the port in the port list to the named RF profile. All ports in the port list must have the same wireless port version.
config wireless ports <portlist> interface [1   2] security-profile <name>	Attaches the ports in the port list to the named security profile. All ports in the port list must have the same wireless port version.
config wireless ports <portlist> interface [1   2] channel	Configures a channel for the specified interface. Default is <code>Auto</code> for both interfaces.
config wireless ports <portlist> interface [1   2] power-level	Configures the power level for the specified interface (full, half, min, one-eighth, quarter). Default is <code>full</code> .
config wireless ports <portlist> interface [1   2] transmit-rate	Configures a transmission rate for the specified port. Choice of rates depends upon the mode of the interface (A or G). Default is <code>54Mbps</code> .
enable   disable wireless ports <portlist> interface [1   2]	Enables or disables the specified port interface.
reset wireless ports <portlist> interface [1   2]	Forces the wireless port interface to reset.

## Managing Wireless Clients

Table 26 lists the commands for configuring interactions with client stations.

**Table 26:** Client Configuration Commands

Command	Description
show wireless ports <portlist> interface [1   2] clients {detail}	Shows wireless client status.
show wireless ports <portlist> interface [1   2] pae-diagnostics	Lists EAP diagnostics for the selected port and interface.
show wireless ports <portlist> interface [1   2] pae-statistics	Lists EAP statistics for the selected port and interface.

## Show Commands

Use the show commands listed in Table 27 to display information on port configuration, RF profiles, security profiles, and stations.

**Table 27:** Show Commands

Command	Description
show wireless ports <portlist> interface [1   2] rf-status {detail}	Lists data rates, and ESS name for the selected port and interface.
show wireless ports <portlist> interface [1   2] security-status {detail}	Lists WEP, authentication, dot1x, and guest mode information for the selected port and interface.
show wireless config	Lists the country, type of management access, management VLAN, and gateway.



**Table 27:** Show Commands (continued)

Command	Description
show wireless ports <portlist> interface [1   2] configuration {detail}	Summarizes wireless configuration information for the selected port and interface.
show wireless ports <portlist> interface [1   2] stats	Lists 802.11 interface statistics for the selected port and interface.
show wireless ports <portlist> interface [1   2] status	Gives the current state of the selected port and interface.

## Event Logging and Reporting

The Summit 300-48 switch supports the following enhancements for wireless event logging and reporting:

- All wireless-related syslog messages are clearly labeled with the wireless port on which the event occurred and the MAC address of the station associated with the event.
- Enumerated type fields are included in syslog messages for filtering by external tools.
- An additional CLI command is included for more granularity (`show wireless ports <portlist> log`).



# 7

## Unified Access Security

---

This chapter describes the security features of the Summit 300-48 switch and includes information on the following topics:

- Overview of Security on page 83
- User Access Security on page 84
- Network Security Policies on page 87
- Network Security Policies on page 87
- CLI Commands for Security on the Switch on page 89

### Overview of Security

The Extreme Unified Access™ Security architecture provides secure access for all wired and wireless stations within the unified network. You can maintain the network with a single, unified security policy, provide service to all stations without requiring upgrades, and take advantage of integrated policy and management capabilities not available in overlay networks or those with “thick” access points. Unified Access Security provides the following key capabilities:

- Consolidated management — Up to 48 wireless ports from a single Summit 300-48 switch, larger network support with less management overhead
- Scalable encryption — ASIC based AES encryption, WPA with TKIP support, and RC4 based WEP support on the Altitude 300 wireless port
- 802.1x Authentication — 802.1x authentication (PEAP, EAP-TTLS, EAP-TLS)

The unified structure simplifies security policies without compromising protection and provides the following benefits:

- Single user experience — Same authentication procedures for wired and wireless users
- Unified management — Single management platform for wired and wireless networks
- Unified configuration — Consistent CLI for wired and wireless functions
- Single authentication infrastructure — Single set of policies, RADIUS, and certificate servers

These security features provide protection for users and for the network infrastructure.

# User Access Security

Effective user security meets the following objectives:

- Authentication — Assuring that only approved users are connected to the network at permitted locations and times.
- Privacy — Assuring that user data is protected.

## Authentication

The authentication process is responsible for screening users who attempt to connect to the network and granting or denying access based on the identity of the user, and if needed, the location of the client station and the time of day. The authentication function also includes secure encryption of passwords for user screening.

For an authentication scheme to be practical and effective, it must be compatible with the currently-installed client software base. That requires accommodating multiple versions of software, including legacy systems with older generation security support. It also requires a strong encryption structure that can be managed across the network as a whole. Authentication should be mutual, with client-to-network authentication and network-to-client authentication. Finally, authentication requires the appropriate authentication servers.

The Unified Access Architecture provides authentication methods that meet all these requirements, while also permitting flexibility in selecting the options appropriate to your specific network environment.

### Authentication Method: Open

The wireless network consisting of the Summit 300-48 switch and Altitude 300 wireless port supports 802.11 open system authentication, in which the station identifies the SSID. Although open authentication may be acceptable for the wired networks, hacking tools can easily obtain this information on the wireless side, rendering open authentication virtually useless for the enterprise wireless network.

### Authentication Method: WEP

Wired Equivalency Privacy (WEP) is the first generation security option for 802.11 networks and includes both an authentication and encryption mechanism. It uses a set of authentication keys and the RC4 security algorithm. Unfortunately, weaknesses in the encryption scheme have left the method open to theft of login and password information and, consequently, to compromise of the authentication process. WEP is best used as part of a multi-tiered security scheme and in legacy environments.

### Authentication Method: 802.1x/EAP

Extensible Authentication Protocol (EAP) provides numerous improvements over earlier generation authentication methods. The 802.1x specification incorporates these as implemented directly on Ethernet. In 802.1X/EAP authentication, the user's identity, not MAC address, is the basis for authentication. When the user requests access to the wireless port, the access point forces the user's station into an unauthorized state. In this state, the client station sends an EAP start message. The switch responds with a request for the user identity, which it passes to a central authentication server. The server software authenticates the user and returns an permit or deny message to the switch, which

then extends or denies access as instructed, and passes along configuration information such as VLAN and priority.

802.1x supports several EAP-class advanced authentication protocols, which differ in the specific identification types and encryption methods for the authentication:

- EAP-TLS (Transport Layer Security) — Performs mutual authentication using security certificates. Good for wired and wireless networks
- EAP-TTLS (Tunneled TLS) — Extends TLS flexibility and is compatible with a wide range of authentication algorithms. Good for wired and wireless networks
- PEAP (protected EAP) — Is compatible with a wide range of authentication algorithms. Good for wired and wireless networks

802.1x security is compatible with legacy 802.1x and with newer clients that support WPA based 802.1x. It is possible to configure both versions (legacy and WPA) on the same Summit 300-48 switch port. When a client associates to the Summit 300-48 switch port, it indicates 802.11 open authentication. Then if 802.1x is enabled on the port, the client is able to associate, and further authentication is performed. If the authentication is successful, the backend RADIUS server optionally specifies a VLAN tag using Vendor Specific Attributes in the Access Accept message.

### Location Based Authentication

Location-based authentication restricts access to users in specific buildings. The Summit 300-48 switch sends the user's location information to the RADIUS server, which then determines whether or not to permit user access. When you configure a location field, the information is sent out in RADIUS Access Request packets as a VSA and can be used to enforce location-based policies.

### Time-Based Authentication

Time-based authentication restricts access to users to certain dates or times. The Radius server can determine policies based on the time of day when the Authentication request is received from the Summit 300-48 switch.

### Privacy

Privacy refers to the protection of user data sent over the network. It is a major concern in wireless network, since physical security is not possible for data sent over wireless links. While encryption is the major component of a privacy solution, an effective approach also requires management of encryption keys, integrity checks to protect against packet tampering, and ability to scale as the network grows.

To isolate all traffic using WEP and help improve the security of the overall network, the Summit 300-48 switch classifies all traffic using shared authentication into a separate WEP VLAN. This VLAN is configured using a security profile.

### Cipher Suites

Table 28 lists several cipher suites that standards organizations have identified to group security capabilities under a common umbrella. The Extreme Unified Security Architecture supports or will

incorporate each of these suites, and the Altitude 300 wireless port supports hardware-based AES and RC4 encryption.

**Table 28:** Wi-Fi Security Cipher Suites

Name	Authentication	Privacy	Sponsoring Organization
WEP	None or MAC	WEP/RC4	IEEE
WPA	802.1x	TKIP/RC4	Wi-Fi Alliance
WPA	802.1x	CCMP/AES/TKIP	IEEE

### WPA-Only Support

To support WPA clients, the Summit 300-48 switch port sets the privacy bit in the beacon frames it advertises. The switch also advertises the set of supported unicast and multicast cipher suites and the configured and supported authentication modes as part of the association request. If the switch advertises the cipher suites and authentication modes, then the client is able to associate with the wireless port and is subject to further authentication and key derivation. If the cipher suites and authentication modes are not advertised, then the client cannot associate with the wireless port.

WPA support is compatible with 802.1x authentication or pre-shared keys. With pre-shared keys, key derivation and distribution are done using the EAPOL-KEY messages. All clients that indicate PSK are assigned to the PSK VLAN, which is configured on the Summit 300-48 switch port. The switch advertises this information using WPA IEs.

### Legacy and WPA 802.1x Support

It is possible to support WEP40 and WEP104 as unicast cipher suites along with legacy and WPA-based clients. You can configure the WEP options independently of the AES and TKIP options used for WPA. The multicast uses the lowest WEP suite. The switch advertises the set of unicast cipher and multicast suites using WPA IEs. <sup>1</sup>

If dot1x authentication is set to `all` and the same VLAN is used for WPA and legacy clients, then session key derivation and distribution takes place independently. For multicast keys, the legacy 802.1x is now used for all clients. When legacy and WPA clients are supported simultaneously, group key updates are disabled.

When Legacy 802.1x and WPA clients are both allowed access, then a different set of keys are used for legacy clients and for WPA clients. WPA clients can use AES and TKIP encryption, while legacy clients use WEP encryption. The multicast cipher can be set to AES, TKIP, or WEP, in which case the unicast cipher used by WPA clients will be AES, TKIP, and WEP respectively.



#### NOTE

*Legacy and WPA clients should not be put on the same VLAN.*

1. 40-bit WEP encryption is sometimes called 64bit (40+24IV), and 104-bit encryption is sometimes called 128bit (104+24IV).

# Network Security Policies

Network security policy refers to a set of network rules that apply to user access. You can base the rules on a variety of factors, including user identification, time and location, and method of authentication. It is possible to design network security policies to do all of the following:

- Permit or deny network access based on location and time of day.
- Place the user into a VLAN based on identity or authentication method.
- Limit where the user is permitted to go on the network based on identity or authentication method .

## Policy Design

When designing a security policy for your network, keep the following objectives in mind:

- Make each wired and wireless client as secure as possible.
- Protect company resources.
- Make the network infrastructure as secure as possible.
- Be able to track and identify wired and wireless rogues.

To achieve these objectives, it is necessary to work within the constraints of your environment:

- Technology of all the clients
  - 802.11 radio technology (b, a, g, a/b, a/g)
  - Operating system (W2K, XP, Pocket PC, ....)
  - Client readiness for 802.1x; client upgrades
- Authentication servers available or planned
  - Operating System Login only (i.e. Domain Access, LDAP)
  - RADIUS for Users
  - PKI Infrastructure
- Nature of the user population
- Ability to divide users into meaningful groups
- Network resources required by users
- Desired access restrictions based on resources, locations, times, and security level
- Acceptable level of network management and user training
- Anticipated changes in the network

## Policy Examples

The following examples suggest typical uses of network security policies.

**Example.** You want to give employees complete network access but limit access to visitors. The solution is to base network access on the authentication method, as indicated in Table 29.

**Table 29:** Authentication-Based Network Access Example

Authentication Method	User Placement
802.1x with dynamic WEP	Internal VLAN
TKIP with pre-shared keys	PSK VLAN
WEP	WEP VLAN
Fails 802.1x authentication	Deny access



### NOTE

*Not all methods can be used at the same time on the same interface.*

**Example.** You want to restrict user access to certain locations or times. The solution is to include the access point as a component of network access and include time restrictions for certain locations.

## Policies and RADIUS Support

The authentication features of the Summit 300-48 switch are tightly integrated with RADIUS. You can specify the following types of RADIUS access control policies:

- **User-based** — 802.1x requests provide the RADIUS server with the user name and password. Based on the user name, the RADIUS server sends back authentication information, including allow/deny, assigned VLAN, and VLAN tag.
- **Location-based** — You can configure a location string for each wireless port. The location is sent to the RADIUS server as a vendor-specific attribute. The RADIUS server uses this information to determine the access policy.

## RADIUS Attributes

Table 30 lists the attributes are included in each request for access:

**Table 30:** RADIUS Request Attributes

Attribute	Description
User-Name	User name for dot1x or MAC address
User-Password	User-specified for dot1x or blank
Service-Type	Value is login (1)
Vendor-Specific	Contains EXTREME_USER_LOCATION, and the value is as configured by the user for the location of each wireless port



Table 31 lists the attributes included in the RADIUS response.

**Table 31:** RADIUS Response Attributes

Attribute	Description
EXTREME_NETLOGIN_VLAN_TAG	VLAN for this MAC

### Vendor-Specific Attributes

Table 32 lists the supported vendor-specific attributes (VSAs). The Extreme vendor ID is 1916.

**Table 32:** Vendor-Specific Attributes

VSA	Attribute Value	Type	Sent In
EXTREME_NETLOGIN_VLAN_TAG	209	Integer	Access-accept
EXTREME_USER_LOCATION	208	String	Access-request

The following rules apply for VSAs:

- There is no RADIUS support required for WEP authentication.
- For locations, the switch receives Extreme VSA containing the location of the access point. The RADIUS server uses the location VSA to determine whether to allow or deny access.
- For WPA and legacy dot1x clients, the RADIUS server sends the VLAN value to use for the client.

## CLI Commands for Security on the Switch

### Security Profile Commands

Table 33 lists the CLI commands for creating security profiles.

**Table 33:** Security Profile Commands

Command	Description
create security-profile <name> {copy <name>}	Creates a new profile identified by the string name. Optional from argument specifies the name of an existing profile from which the system copies the initial values
delete security-profile <name>	Deletes the named security profile. The named profile must not be currently attached to any active port on the switch.
config security-profile <name> <property> <value>	Sets the value of the property specified in the command line. Changes take effect immediately and are propagated to all ports sharing the named profile. If the command fails, none of the changes is propagated to any of the ports. Table 34 lists the <property> values.
show security-profile {<name>}	Shows the configured parameters of the security profile.

Table 34 lists the properties for the security profile configuration command.

**Table 34:** Security Profile Command Property Values

Case	Default	Ranges	Action
ssid-in-beacon <value>	on	off   on	Turns on whether the SSID is published in the beacon or not. If you set this to <code>off</code> then the beacon does not contain the SSID and the client must know the SSID before it can associate. Sniffing on the beacon shows an empty SSID.
wep authentication <value> {vlan <vlan_name>}	off	off   on	Enables open vs. shared authentication. Setting this to <code>on</code> sets the interface for shared authentication. Note that WEP authentication must be on in order to use wep encryption. (Open authentication with WEP encryption is not supported). The VLAN must be specified only if WEP authentication is on. All WEP traffic gets classified into this VLAN if WEP is on.
wep default-key-index <index>	0	0-3	Sets the index of the WEP key. The key at the specified index must be configured before you can set the default index for WEP auth/encryption.
encryption-length	128	64   128	Sets the length of the encryption key used for WEP or legacy dot1x clients. For legacy dot1x clients, the switch generates a random key based on the given length and WEP encryption. WPA clients use TKIP   AES as their cipher suite. This command can be issued only if WEP authentication is <code>on</code> or if dot1x authentication is <code>all</code> (dot1x authentication properties below).
wep key add <0-3> [hex <hexoctets>   plaintext <string>]	hex	type: hex   plaintext	Adds the given WEP key at the given index. This key is used for WEP encryption as well as for EAP-MD5. If you use hex mode, then the key should be made up of hex digits (i.e. if encryption-length is 64 the key should be 10 hex digits (64-24 (ICV) = 40bits = 5 bytes = 10 hex digits). When you specify plaintext mode, the key is simply the ascii value of the letters in the specified key (i.e. A = 35 and so on...). Note that plaintext does not mean passphrase.
wep key del <integer>	0	0-3	Deletes the specified WEP key. When you delete a WEP key whose index is the default WEP key index, then the default index is changed automatically to the lowest specified WEP key (or N/A if no WEP keys have been specified).
dot1x authentication <value>	none	all   none   wpa	Enables dot1x authentication. Setting dot1x to <code>all</code> implies legacy clients are allowed (plain dot1x as well as WPA). Setting dot1x authentication to <code>rsn</code> only allows WPA clients. Setting dot1x to <code>None</code> will disable dot1x.

**Table 34:** Security Profile Command Property Values (continued)

Case	Default	Ranges	Action
dot1x multicast-cipher <value>	wep	aes   tkip   wep	Specifies the cipher suite to use for legacy 802.1x or WPA clients. If the mcast cipher suite is <code>aes</code> , then the unicast cipher suite is AES. If the mcast cipher suite is <code>tkip</code> or <code>wep</code> , the unicast cipher suite is TKIP. Specifying this has no effect if non-WPA clients are used. If non-WPA clients are used, then WEP encryption is used for both unicast and broadcast. The key length for non-WPA clients is specified using the <code>encryption-length</code> property above. Also, if both WPA and non-WPA clients are on the same VLAN, then the packet is broadcast twice (once with each encryption key).
dot1x auth-suite dot1x			Sets the authentication suite to be dot1x, which means that keys are dynamically generated. Keys are not pushed from the RADIUS server, but are generated on the access point. This is valid only for WPA clients.
dot1x auth-suite psk pre-shared-key <value> <string> vlan <vlan name>		hex   plaintext   passphrase	Specifies pre-shared keys to be the authentication-suite for dot1x. The key can be specified as a hex key or passphrase or plaintext. Plaintext keys are converted to hex keys by using the ASCII values of the various characters in the key. The length of the key must 32 bytes (64 hex digits, or 32 characters when using plaintext keys). For passphrases, the key must be at least 8 characters long. All clients authenticated using this policy are placed into the specified VLAN.
dot1x group-update-timer <integer>	1	1-1440	Specifies the time used to re-key the broadcast key (in minutes).
dot1x pairwise-update-timer <integer>	1	1-1440	Specifies the time interval at which session keys are refreshed (in minutes).
dot1x reauth-period <integer>	3600	60-60,000	Specifies the time interval (in seconds) at which the clients will need to re-authenticate.

## Example Wireless Configuration Process

This section provides an example of the configuration process. First, the wireless management VLAN is configured, IP addresses are assigned, and RF profiles are created and configured. Next, the security profile is created, with examples given for WEP and dot1x security. Finally, example steps are provided for assigning profiles to ports.



### NOTE

*The commands provided in each step are examples.*

To configure the VLAN, addresses, and RF profiles, follow these steps:

- 1 Create the wireless management VLAN.

```
create vlan wireless-mgmt
```

- 2 Remove the wireless port from the default VLAN.

```
configure vlan default delete ports 1:5
```

- 3 Add the wireless port to the management VLAN.

```
configure vlan wireless-mgmt add ports 1:5
```

- 4 Configure this VLAN as the management VLAN.

```
configure wireless vlan wireless-mgmt
```

- 5 Assign an IP address to the VLAN.

```
configure vlan wireless-mgmt ip-address 192.168.0.1
```

- 6 Assign an IP address on the VLAN for each wireless port (port 1:5 in the example).

```
configure wireless port 1:5 ip-address 192.168.0.105
```

- 7 Create an RF profile for the A interfaces by copying from the default profile.

```
create rf-profile RF_A copy DEFAULT_A
```

- 8 Assign a network name (ess-name) to the RF-profile for the A interface.

```
configure rf-profile RF_A ess-name 80211_A
```

- 9 Create an RF profile for the G interfaces by copying from the default profile.

```
create rf-profile RF_G copy DEFAULT_G
```

- 10 Assign network name (ess-name) to the RF-profile for the G interface.

```
configure rf-profile RF_G ess-name 80211_G
```

To configure WEP security, follow these steps:

- 1 Create a security profile (wep-secure) by copying from the default unsecure profile.

```
create security-profile wep-secure copy unsecure
```

- 2 Create a WEP VLAN. This is the VLAN in to which all WEP traffic will be classified.

```
create vlan wep-vlan
```

- 3 Configure the tag for the WEP VLAN

```
configure vlan wep-vlan tag 10
```

- 4 Add the wireless port to be a tagged port on the WEP-VLAN. The port can be a tagged port or an untagged port of the WEP VLAN. If the port is a tagged port, the traffic flowing from the AP to the switch will be tagged with the specified VLAN, else it will be untagged.

```
configure vlan wep-vlan add ports 1:5 tagged
```

- 5 Turn on WEP authentication in this security profile and assign the VLAN.

```
configure security-profile wep-secure wep authentication on vlan wep-vlan
```

- 6 Configure the security profile for WEP encryption length of 64.

```
configure security-profile wep-secure encryption-length 64
```

- 7 Configure the first WEP key (0) with the hex encryption code 1234567891.

```
configure security-profile wep-secure wep key add 0 hex 1234567891
```

If you enter the wrong number of characters for the code, a message similar to the following appears.

```
Invalid number of bytes in key. Expected 10 bytes, got 15 bytes.
```

- 8** Configure the security profile to use the 0 key you just defined as the default encryption key.

```
configure security-profile wep-secure wep default-key-index 0
```

To configure dot1x security, follow these steps:

- 1** Create a security profile (dot1x-secure) by copying from the default unsecure profile.

```
create security-profile dot1x-secure copy unsecure
```

- 2** Configure the security profile for all levels of dot1x authentication.

```
configure security-profile dot1x-secure dot1x authentication all
```

- 3** Configure the security profile with the dot1x authentication suite.

```
configure security-profile dot1x-secure dot1x auth-suite dot1x
```

- 4** Configure the security profile to use WEP as the cipher method for multicast messages. This automatically applies to unicast messages as well.

```
configure security-profile dot1x-secure dot1x multicast-cipher wep
```

- 5** Configure an encryption length of 128 for the security profile. You also need to configure the RADIUS server for dot1x authentication. There is a special command `enable radius wireless` to enable radius for wireless access. See “Policies and RADIUS Support” on page 88 for more information.

```
configure security-profile dot1x-secure encryption-length 128
```

To assign profiles to ports, follow these steps:

- 1** Configure interface 1 on port 1:5 to use the RF profile `RF_A`.

```
configure wireless ports 1:5 interface 1 rf-profile RF_A
```

- 2** Configure interface 2 on port 1:5 to use the RF profile `RF_G`.

```
configure wireless ports 1:5 interface 2 rf-profile RF_G
```

- 3** Configure interfaces 1 and 2 on port 1:5 to use the `wep-secure` security profile or the `dot1x-secure` security profile.

```
configure wireless ports 1:5 interface 1 security-profile wep-secure
```

```
configure wireless ports 1:5 interface 2 security-profile wep-secure
```

OR

```
configure wireless port 1:5 interface 1 security-profile dot1x-secure
```

```
configure wireless port 1:5 interface 2 security-profile dot1x-secure
```

- 4** Configure the channel on the A and the B interface. Specifying 0 as the channel indicates that the least interfering channel should be selected by the interface.

```
configure wireless ports 1:5 interface 1 channel 0
```

```
configure wireless ports 1:5 interface 2 channel 11
```





# Power Over Ethernet

---

This chapter explains how to configure the Summit 300-48 switch to supply power to devices using the Power over Ethernet (PoE) capability. It contains the following sections:

- Overview on page 95
- Port Power Management on page 96
- Per-Port LEDs on page 98
- Configuring Power Over Ethernet on page 98

## Overview

Power over Ethernet (PoE), defined by the IEEE 802.3af specification, is an effective method of supplying 48 VDC power to certain types of powered devices (PDs) by way of Category 5 or Category 3 twisted pair Ethernet cables. Devices include the Altitude 300 wireless port. IP telephones, laptop computers, web cameras, or other devices. With PoE, a single Ethernet cable supplies power and the data connection, thereby saving time and expense associated with separate power cabling and supply.

The 802.3af specification for PoE includes a method of detection to assure that power is delivered only to devices that meet the specification.

## Summary of PoE Features

The Summit 300-48 switch supports the following PoE features:

- Configuration and control of the power distribution for PoE at the system (slot) level
- Configuration and control of the power distribution for PoE at the port level
- Real time detection of powered devices on the line
- Monitor and control of fault conditions
- Support for both human interface and machine interface for configuration and monitoring of status at the port level
- Management of an over-subscribed power budget
- LED control for indicating the port “power” state

## Port Power Management

When you connect PDs, the Summit 300-48 switch automatically discovers and classifies those that are AF-compliant. The following functions are supported for delivering power to the port:

- Enabling the port for discovery and classification
- Enabling power delivery to a discovered device
- Enforcing port power limits by denying power to a device that exceeds the power limit
- Enforcing class limits by denying power to a device that exceeds the class limit
- Reporting and tracking port power faults
- Managing power budgets and allocation
- Managing port priorities

### Port Power Operator Limit

Each port is configured by default to permit AF-compliant devices and to cause a fault for any device that exceeds the power level defined for the device class. You can also specify a power limit on a per-port basis. Power is allowed up to maximum limit (20 watts). There are several options for defining a violation policy and creating a device fault:

- Class violation—Power is removed if the PD consumes more than the discovered class limit.
- Operator limit—Power is removed if the PD consumes more than the operator-specified limit.
- Maximum of operator limit and class—Power is removed if the PD consumes more than the operator limit or discovered class limit, whichever is greater.
- None—Power is removed if the device exceeds the maximum limit of 20 watts.

### Power Budget Management

The Summit 300-48 switch software is responsible for managing overall power consumption to ensure that it does not attempt to delivery more power than is available. You can configure how the Summit 300-48 switch allocates power to devices upon power-up and in the event that available power is reduced.

#### Reserved Power

You can reserve power for devices connected to a specific port. When a new device is discovered, its defined power requirement is first subtracted from the reserved power pool. If there is sufficient reserved power on the port, the device is powered. Otherwise the remaining power is subtracted from the common pool, and the device is powered if there is sufficient reserved plus common power available. Reserved power is subtracted from the common pool and unavailable to other ports. The total reserved power cannot exceed the total available power.



#### NOTE

*A connected device may draw more power than the amount reserved, due to configuration error or oversight. The switch provides notification if this occurs.*



## Common Power Pool

The common power pool represents the total amount of power available on a per-slot basis, less any power reserved or allocated to currently powered devices. When a new device is discovered, its defined power requirements are subtracted from the common power pool. If the common pool does not have sufficient available power, power is not supplied to the device. In this case, the port is placed in a power-denied state. The device can be powered at a later time if more power becomes available to the common power pool due to another device disconnecting or if previously reserved power becomes available.

If multiple devices are in the denied state and more power becomes available, the devices are powered in order of priority and connection.

## Port Connection Order

The Summit 300-48 switch software tracks the order of connection for powered devices. The connection order is recorded at the time a device is first discovered and classified. The connection order is reset if the device is disconnected. This connection order is maintained even if the switch is powered down or power is interrupted, and the device must be discovered again.

During system startup, ports are powered initially based only on the connection order. During normal system operations, port power order is determined first based upon priority, then discovery time. Thus, the highest priority port with the earliest discovery time is powered first.

## Port Power Priorities

You can set the priority of a port to low, high, or critical. Higher priority ports are given precedence in powering sequence.

## Port Power Reset

You can set ports to experience a power-down, discover, power-up cycle without returning the power to the common pool. This allows you to reset powered devices without losing their claim to the common power pool or connection order.

## Port Power Events

If a port has sufficient reserved power for a newly discovered and classified device, the device receives power. If additional power is required and the common pool has sufficient available power, the device is powered and the incremental power is subtracted from the common pool. If the port does not have reserved power, but sufficient power is available from the common pool, the power is subtracted from the pool.

Port power budget is determined based upon the maximum class power levels or operator specification, not actual consumed power. For example, if a port is configured with an operator limit of 20 watts and the violation precedence is set to the operator limit, then 20 watts is budgeted for the port even if a 5 watt 802.3af compliant device is connected.

If a sufficient mix of reserved and common power is not available, the port enters a denied state and is not given power.

Ports are powered based upon their priority and discovery time. Higher priority ports with the oldest discovery time are powered first.

If a device consumes more power than it is allocated by class type, it is considered a class violation. The device enters a fault state, and unreserved power is returned to the common pool. Power is also returned to the common pool if a port is disconnected. The device stays in the fault state until you explicitly clear the fault, disable the port for power, or disconnect the device.

## Per-Port LEDs

The per-port LEDs indicate link and power status for PoE usage, as indicated in Table 35:

**Table 35:** Per-Port LEDs

	Port Disabled	Link Up	Link Down	Activity
Non-powered device	off	solid green	off	blinking green
Device powered	blinking amber	solid amber	amber/green	blinking amber
Power Fault	amber/green	amber/green	amber/green	amber/green



### NOTE

*Wait for the LED to extinguish before reconnecting to the port.*

## Configuring Power Over Ethernet

Use the inline power commands in Table 36 to configure PoE on Summit 300-48 switch ports.



### NOTE

*Configuration parameters affecting operational parameters require the port or slot to be first disabled.*

**Table 36:** Power Over Ethernet Configuration Commands

Command	Description
enable inline-power	Enables/disables PoE on the switch. Controls whether inline power will be provided to the system. Setting the value to disable will shutdown power currently provided on all ports on all slots. Default is enable.
disable inline-power	
enable inline-power slot <slotid>	Enables/disables PoE support for the power supply in the indicated slot. Controls whether inline power will be provided to a specific slot. In order for any of the ports to be powered, The system must be enabled for power, the slot must be enabled for power, and the ports must be enabled for power. Default is enable.
disable inline-power slot <slotid>	

**Table 36:** Power Over Ethernet Configuration Commands (continued)

Command	Description
enable inline-power ports <portlist>	Enables PoE for the listed ports.
disable inline-power ports <portlist>	Disables PoE for the listed ports.
config inline-power usage-threshold <threshold>	Sets the threshold for initiation of an alarm should the measured power exceed the threshold. At present, this alarm threshold is shared between the system level utilization and the allocated power budget per slot. If either level goes above the threshold level an alarm will be set.
clear inline-power connection-history slot <slot_number>	Clear the port connection history for the specified slot.
config inline-power budget <watts> slot <slot_number>	Configures amount of power available for inline-power on the slot. Reducing the amount of power available requires the slot to be disabled first.
unconfig inline-power usage-threshold	Resets the threshold back to the default.
config inline-power label <string> ports <portlist>	Provides a user-controllable label to the power port.
config inline-power operator-limit <milliwatts> ports <portlist>	Sets the power limit on the specified port(s) to either the default value or the specified watts. Range is 3000-20000 mW. Default value is 15400 mW minimum according to IEEE 802.3af. This command is used in conjunction with the violation precedence and has no affect if either none or advertised-class is selected for violation precedence.
config inline-power disconnect-precedence [lowest-priority   deny-port]	Controls the disconnect function of power management. When the power drain exceeds the available power budget, due to a rise in power consumption after power is allocated to the ports, the PoE controller disconnects one of the ports to prevent overload on the power supply. There are two controls: <ul style="list-style-type: none"> <li>• lowest-priority—next port connected causes a shutdown of the lowest priority port.</li> <li>• deny-port—next port is denied power, regardless of priority.</li> <li>• The default is deny-port.</li> </ul>

**Table 36:** Power Over Ethernet Configuration Commands (continued)

Command	Description
unconfig inline-power disconnect-precedence [lowest-priority   deny-port]	<p>Returns the <code>disconnect-precedence</code> to the default state of <code>deny-port</code>. When the power drain exceeds the available power budget, due to a rise in power consumption after power is allocated to the ports, the PoE controller disconnects one of the ports to prevent overload on the power supply. There are two controls:</p> <ul style="list-style-type: none"> <li>• <code>lowest-priority</code>—next port connected causes a shutdown of the lowest priority port.</li> <li>• <code>deny-port</code>—next port is denied power, regardless of priority.</li> <li>• The default is <code>deny-port</code>.</li> </ul>
config inline-power violation-precedence [advertised-class   operator-limit   max-class-operator   none] ports <portlist>	<p>Sets the violation precedence for the specified ports. A value of <code>advertised-class</code> will remove/deny power in the case an 802.3af compliant PD consumes power beyond its advertised class limit. There are three controls:</p> <ul style="list-style-type: none"> <li>• <code>operator-limit</code>—removes/denies power if the PD consumes power beyond the configured <code>operator-limit</code>.</li> <li>• <code>max-class-operator</code>—removes/denies power if the PD consumes power beyond the maximum of the detected class limit and the <code>operator-limit</code>.</li> <li>• <code>none</code>—removes/denies power in case the PD device exceeds the maximum allowable wattage according to regulatory maximum of 20,000 mW. The default is <code>max-class-operator</code>, which allows operation of 802.3af compliant PDs.</li> </ul>
config inline-power reserved-budget <milliwatts> ports <portlist>	<p>Sets the reserved power on the specified port(s) to either the default value or the specified watts. Range is 0 or 3000-20000 mW. The default value is 0 mW. Total power reserved may be up to but not greater than the total power for the card. If all of the power available to the card is reserved, then the common power pool is empty.</p>
clear inline-power fault ports <portlist>	<p>Clears the fault condition on the specified ports.</p>
reset inline-power ports <portlist>	<p>Power cycles the specified ports. Ports are immediately de-powered and re-powered, maintaining current power allocations.</p>
config inline-power detection [auto   discovery-test-only] ports <portlist>	<p>Controls the power detection mechanism on the port. Test mode forces power discovery operations, however power is not supplied to detected PDs.</p>
unconfig inline-power detection ports <portlist>	<p>Resets the power detection scheme to the default.</p>

**Table 36:** Power Over Ethernet Configuration Commands (continued)

Command	Description
unconfig inline-power operator-limit ports <portlist>	Resets the operator limit back to the default.
unconfig inline-power violation-precedence ports <portlist>	Resets the violation precedence back to the default.
unconfig inline-power reserved-budget ports <portlist>	Resets the reserved budget back to the default (0 milliwatts).
config inline-power priority [low   high   critical] ports <portlist>	Configures the port priority. Power allocation is provided first to higher priority ports. The default value is low.
unconfig inline-power priority ports <portlist>	Resets the port priority to the default (low).
clear inline-power stats <slot:port>	Clears inline power stats on the specified ports.

**Table 37:** PoE Show Commands

Command	Description
show inline-power	Displays inline power status information for the system.
show inline-power configuration port <portlist>	Provides inline power information for the specified port(s).
show inline-power slot <slotlist>	Provides inline configuration information for the specified slot(s).
show inline-power stats slot <slotlist>	Provides inline power statistics for the specified slot(s). Prints out how many ports are faulted, powered, and waiting for power for the slot.
show inline-power configuration slot <slotlist>	Provides power configuration for each slot.
show inline-power info [detail] port <portlist>	Provides power configuration details for the port.
show inline-power stats port <portlist>	Shows status of power for the port.



# 9

## Forwarding Database (FDB)

---

This chapter describes the following topics:

- Overview of the FDB on page 103
- Configuring FDB Entries on page 105
- Displaying FDB Entries on page 106

### Overview of the FDB

The switch maintains a database of all media access control (MAC) addresses received on all of its ports. It uses the information in this database to decide whether a frame should be forwarded or filtered.

### FDB Contents

Each FDB entry consists of the MAC address of the device, an identifier for the port on which it was received, and an identifier for the VLAN to which the device belongs. Frames destined for devices that are not in the FDB are flooded to all members of the VLAN.

### FDB Entry Types

The Summit 300-48 switch supports up to 8,191 layer 2 FDB entries and 2,047 layer 3 FDB entries. The following are four types of entries in the FDB:

- **Dynamic entries** — Initially, all entries in the database are dynamic. Entries in the database are removed (aged-out) if, after a period of time (aging time), the device has not transmitted. This prevents the database from becoming full with obsolete entries by ensuring that when a device is removed from the network, its entry is deleted from the database. Dynamic entries are deleted from the database if the switch is reset or a power off/on cycle occurs. For more information about setting the aging time, refer to “Configuring FDB Entries” later in this chapter.
- **Nonaging entries** — If the aging time is set to zero, all aging entries in the database are defined as static, nonaging entries. This means that they do not age, but they are still deleted if the switch is reset.
- **Permanent entries** — Permanent entries are retained in the database if the switch is reset or a power off/on cycle occurs. The system administrator must make entries permanent. A permanent entry can either be a unicast or multicast MAC address. All entries entered by way of the command-line

interface are stored as permanent. The Summit 300-48 switches support a maximum of 128 permanent entries.

Once created, permanent entries stay the same as when they were created. For example, the permanent entry store is not updated when any of the following take place:

- A VLAN identifier (VLANid) is changed.
  - A port mode is changed (tagged/untagged).
  - A port is deleted from a VLAN.
  - A port is disabled.
  - A port enters blocking state.
  - A port QoS setting is changed.
  - A port goes down (link down).
- **Blackhole entries** — A blackhole entry configures the switch to discard packets with a specified MAC destination address. Blackhole entries are useful as a security measure or in special circumstances where a specific destination address must be discarded. Blackhole entries are treated like permanent entries in the event of a switch reset or power off/on cycle. Blackhole entries are never aged-out of the database.

## How FDB Entries Get Added

Entries are added into the FDB in the following two ways:

- The switch can learn entries. The system updates its FDB with the source MAC address from a packet, the VLAN, and the port identifier on which the source packet is received.
- You can enter and update entries using a MIB browser, an SNMP Network Manager, or the command-line interface (CLI).

## Associating a QoS Profile with an FDB Entry

You can associate a QoS profile with a MAC address (and VLAN) of a device that will be dynamically learned. The FDB treats the entry like a dynamic entry (it is learned, it can be aged out of the database, and so on). The switch applies the QoS profile as soon as the FDB entry is learned.



### NOTE

---

*For more information on QoS, refer to Chapter 11.*



# Configuring FDB Entries

To configure entries in the FDB, use the commands listed in Table 38.

**Table 38:** FDB Configuration Commands

Command	Description
clear fdb [{<mac_address>   vlan <name>   ports <portlist>}]	Clears dynamic FDB entries that match the filter. When no options are specified, the command clears all FDB entries.
config fdb agingtime <number>	Configures the FDB aging time. The range is 15 through 1,000,000 seconds. The default value is 300 seconds. A value of 0 indicates that the entry should never be aged out.
create fdbentry <mac_address> vlan <name> ports [<portlist>   all] {{qosprofile <qosprofile> {ingress-qosprofile <qosprofile>}   {ingress-qosprofile <qosprofile>} {qosprofile <qosprofile>}}	Creates a permanent static FDB entry. Specify the following: <ul style="list-style-type: none"> <li>• <code>mac_address</code> — Device MAC address, using colon separated bytes.</li> <li>• <code>name</code> — VLAN associated with MAC address.</li> <li>• <code>portlist</code> — Port numbers associated with MAC address.</li> <li>• <code>qosprofile</code> — QoS profile associated with destination MAC address of the egress port.</li> <li>• <code>ingress-qosprofile</code> — QoS profile associated with the source MAC address of the ingress port.</li> </ul> <p>If more than one port number is associated with a permanent MAC entry, packets are multicast to the multiple destinations.</p>
create fdbentry <mac_address> vlan <name> dynamic {{qosprofile <qosprofile> {ingress-qosprofile <qosprofile>}   {ingress-qosprofile <qosprofile>} {qosprofile <qosprofile>}}	Creates a permanent dynamic FDB entry. Assigns a packet with the specified MAC address and VLAN to a specific QoS profile. If you only specify the ingress QoS profile, the egress QoS profile defaults to none, and vice-versa. If both profiles are specified, the source MAC address of an ingress packet and the destination MAC address of an egress packet are examined for QoS profile assignment.
create fdbentry <mac_address> vlan <name> blackhole {source-mac   dest-mac   both}	Creates a blackhole FDB entry. Specify: <ul style="list-style-type: none"> <li>• <code>source-mac</code> — The blackhole MAC address matches the ingress source MAC address.</li> <li>• <code>dest-mac</code> — The blackhole MAC address matches the egress destination MAC address.</li> <li>• <code>both</code> — The blackhole MAC address matches the ingress source MAC address or the egress destination MAC address.</li> </ul>
delete fdbentry {<mac_address> vlan <name>   all}	Deletes one or all permanent FDB entries.
disable learning port <portlist>	Disables MAC address learning on one or more ports for security purposes. If MAC address learning is disabled, only broadcast traffic, EDP traffic, and packets destined to a permanent MAC address matching that port number, are forwarded. The default setting is enabled.

**Table 38:** FDB Configuration Commands (continued)

Command	Description
enable learning port <portlist>	Enables MAC address learning on one or more ports.

## FDB Configuration Examples

The following example adds a permanent entry to the FDB:

```
create fdbentry 00:E0:2B:12:34:56 vlan marketing port 1:4
```

The permanent entry has the following characteristics:

- MAC address is 00:E0:2B:12:34:56.
- VLAN name is *marketing*.
- Port number for this device is 1:4.

This example associates the QoS profile *qp2* with a dynamic entry that will be learned by the FDB:

```
create fdbentry 00:A0:23:12:34:56 vlan net34 dynamic qosprofile qp2
```

This entry has the following characteristics:

- MAC address is 00A023123456.
- VLAN name is *net34*.
- The entry will be learned dynamically.
- QoS profile *qp2* will be applied when the entry is learned.

## Displaying FDB Entries

To display FDB entries, use the following command:

```
show fdb {<mac_address> | vlan <name> | ports <portlist> | permanent}
```

where the following is true:

- *mac\_address* — Displays the entry for a particular MAC address.
- *vlan <name>* — Displays the entries for a VLAN.
- *ports <portlist>* — Displays the entries for a slot and port combination.
- *permanent* — Displays all permanent entries, including the ingress and egress QoS profiles.

With no options, the command displays all FDB entries.

---

This chapter describes the following topics:

- Overview of Access Policies on page 107
- Using Access Control Lists on page 107

## Overview of Access Policies

*Access policies* are a generalized category of features that impact forwarding and route forwarding decisions. Access policies are used primarily for security and quality of service (QoS) purposes.

The three categories of access policies are:

- Access control lists
- Rate limits

### Access Control Lists

Access control lists are used to perform packet filtering and forwarding decisions on incoming traffic. Each packet arriving on an ingress port is compared to the access list in sequential order and is either forwarded to a specified QoS profile or dropped. These forwarded packets can also be modified by changing the 802.1p value and/or the DiffServe code point. Using access lists has no impact on switch performance.

### Rate Limits

Rate limits are almost identical to access control lists. Incoming packets that match a rate limit access control list are allowed as long as they do not exceed a pre-defined rate. Excess packets are either dropped, or modified by resetting their DiffServ code point.

## Using Access Control Lists

Each access control list consists of an access mask that selects which fields of each incoming packet to examine, and a list of values to compare with the values found in the packet. Access masks can be

shared multiple access control lists, using different lists of values to examine packets. The following sections describe how to use access control lists.

## Access Masks

There are between twelve and fourteen access masks available in the Summit 300-48, depending on which features are enabled on the switch. Each access mask is created with a unique name and defines a list of fields that will be examined by any access control list that uses that mask (and by any rate limit that uses the mask).

An access mask consists of a combination of the following thirteen fields:

- Ethernet destination MAC address
- Ethernet source MAC address
- VLANid
- IP Type of Service (TOS) or DiffServ code point
- Ethertype
- IP protocol
- IP destination address and netmask
- Layer 4 destination port
- IP source address and netmask
- Layer 4 source port, or ICMP type and/or ICMP code
- TCP session initiation bits (permit-established keyword)
- Egress port
- Ingress ports

An access mask can also have an optional, unique precedence number associated with it.

## Access Lists

Each entry that makes up an access list contains a unique name and specifies a previously created access mask. The access list also includes a list of values to compare with the incoming packets, and an action to take for packets that match. When you create an access list, you must specify a value for each of the fields that make up the access mask used by the list.

For packets that match a particular access control list, you can specify the following actions:

- Drop  
Drop the packets. Matching packets are not forwarded.
- Permit-established  
Drop the packet if it would initiate a new TCP session (see, “The permit-established Keyword” on page 111).
- Permit  
Forward the packet. You can send the packet to a particular QoS profile, and modify the packet’s 802.1p value and/or DiffServe code point.

## Rate Limits

Each entry that makes up a rate limit contains a unique name and specifies a previously created access mask. Like an access list, a rate limit includes a list of values to compare with the incoming packets and an action to take for packets that match. Additionally, a rate limit specifies an action to take when matching packets arrive at a rate above the limit you set. When you create a rate limit, you must specify a value for each of the fields that make up the access mask used by the list.



### NOTE

---

*Unlike an access list, a rate limit can only be applied to a single port. Each port will have its own rate limit defined separately.*

For packets that match a particular list, and arrive at a rate below the limit, you can specify the following action:

- Permit
  - Forward the packet. You can send the packet to a particular QoS profile, and modify the packet's 802.1p value and/or DiffServe code point.

For packets that match a particular list, and arrive at a rate that exceeds the limit, you can specify the following actions:

- Drop
  - Drop the packets. Excess packets are not forwarded.
- Permit with rewrite
  - Forward the packet, but modify the packet's DiffServe code point.

The allowable rate limit values for the 100BT ports are 1, 2, 3, 4 ... 100 Mbps, and for the Gigabit ports are 8, 16, 24, 32...1000 Mbps.



### NOTE

---

*The rate limit specified in the command line does not precisely match the actual rate limit imposed by the hardware, due to hardware constraints. See the release notes for the exact values of the actual rate limits, if required for your implementation.*

## How Access Control Lists Work

When a packet arrives on an ingress port, the fields of the packet corresponding to an access mask are compared with the values specified by the associated access lists to determine a match.

It is possible that a packet will match more than one access control list. If the resulting actions of all the matches do not conflict, they will all be carried out. If there is a conflict, the actions of the access list using the higher precedence access mask are applied. When a match is found, the packet is processed. If the access list is of type deny, the packet is dropped. If the list is of type permit, the packet is forwarded. A permit access list can also apply a QoS profile to the packet and modify the packet's 802.1p value and the DiffServe code point.

## Access Mask Precedence Numbers

The access mask precedence number is optional, and determines the order in which each rule is examined by the switch. Access control list entries are evaluated from highest precedence to lowest precedence. Precedence numbers range from 1 to 25,600, with the *number 1 having the highest precedence*. However, an access mask *without* a precedence specified has a higher precedence than any access mask *with* a precedence specified. The first access mask defined without a specified precedence has the highest precedence. Subsequent masks without a specified precedence have a lower precedence, and so on.

## Specifying a Default Rule

You can specify a default access control list to define the default access to the switch. You should use an access mask with a low precedence for the default rule access control list. If no other access control list entry is satisfied, the default rule is used to determine whether the packet is forwarded or dropped. If no default rule is specified, the default behavior is to forward the packet.



### NOTE

*If your default rule denies traffic, you should not apply this rule to the Summit 300-48 port used as a management port.*

The following example shows an access control list that is used to specify an default rule to explicitly deny all traffic:

```
create access-mask ingress_mask ports precedence 25000
create access-list DenyAll ingress_mask ports 1:2-1:26 deny
```

After the default behavior of the access control list has been established, you can create additional entries using precedence numbers.

The following access control list example shows an access control list that will forward traffic from the 10.1.2.x subnet even while the above default rule is in place:

```
create access-mask ip_src_mask source-ip/24 precedence 1000
create access-list TenOneTwo ip_src_mask source-ip 10.1.2.0/24 permit
```

## The permit-established Keyword

The `permit-established` keyword is used to directionally control attempts to open a TCP session. Session initiation can be explicitly blocked using this keyword.



### NOTE

*For an example of using the permit-established keyword, refer to “Using the Permit-Established Keyword” on page 116.*

The permit-established keyword denies the access control list. Having a permit-established access control list blocks all traffic that matches the TCP source/destination, and has the SYN=1 and ACK=0 flags set.

## Adding Access Mask, Access List, and Rate Limit Entries

Entries can be added to the access masks, access lists, and rate limits. To add an entry, you must supply a unique name using the `create` command, and supply a number of optional parameters (see Table 39 for the full command syntax). For access lists and rate limits, you must specify an access mask to use. To modify an existing entry, you must delete the entry and retype it, or create a new entry with a new unique name.

To add an access mask entry, use the following command:

```
create access-mask <name> ...
```

To add an access list entry, use the following command:

```
create access-list <name> ...
```

To add a rate limit entry, use the following command:

```
create rate-limit <name> ...
```

### Maximum Entries

If you try to create an access mask when no more are available, the system will issue a warning message. Three access masks are constantly used by the system, leaving a maximum of 13 user-definable access masks. However, enabling some features causes the system to use additional access masks, reducing the number available.

For each of the following features that you enable, the system will use one access mask. When the feature is disabled, the mask will again be available. The features are:

- IGMP or OSPF (both would share a single mask)
- DiffServ examination
- QoS monitor

The maximum number of access list allowed by the hardware is 254 for each block of eight 10/100 Ethernet ports and 126 for each Gigabit Ethernet port, for a total of 1014 rules (254\*3+126\*2). Most user entered access list commands will require multiple rules on the hardware. For example, a global rule (an access control list using an access mask without “ports” defined), will require 5 rules, one for each of the 5 blocks of ports on the hardware.

The maximum number of rate-limiting rules allowed is 315 (63\*5). This number is part of the total access control list rules (1014).

## Deleting Access Mask, Access List, and Rate Limit Entries

Entries can be deleted from access masks, access lists, and rate limits. An access mask entry cannot be deleted until all the access lists and rate limits that reference it are also deleted.

To delete an access mask entry, use the following command:

```
delete access-mask <name>
```

To delete an access list entry, use the following command:

```
delete access-list <name>
```

To delete a rate limit entry, use the following command:

```
delete rate-limit <name>
```

## Verifying Access Control List Configurations

To verify access control list settings, you can view the access list configuration.

To view the access list configuration use the following command:

```
show access-list {name | ports <portlist>}
```

To view the rate limit configuration use the following command:

```
show rate-limit {name | ports <portlist>}
```

To view the access mask configuration use the following command:

```
show access-mask {name}
```

## Access Control List Commands

Table 39 describes the commands used to configure access control lists.



**Table 39:** Access Control List Configuration Commands

Command	Description
<pre> create access-list &lt;name&gt; access-mask &lt;access-mask name&gt; {dest-mac &lt;dest_mac&gt;} {source-mac &lt;src_mac&gt;} {vlan &lt;name&gt;} {ethertype [IP   ARP   &lt;hex_value&gt;]} {tos &lt;ip_precedence&gt;   code-point &lt;code_point&gt;} {ipprotocol [tcp udp icmp igmp &lt;protocol_num&gt;]} {dest-ip &lt;dest_IP&gt;/&lt;mask length&gt;} {dest-L4port &lt;dest_port&gt;} {source-ip &lt;src_IP&gt;/&lt;mask length&gt;} {source-L4port &lt;src_port&gt;   {icmp-type &lt;icmp_type&gt;} {icmp-code &lt;icmp_code&gt;}} {egressport &lt;port&gt;} {ports &lt;portlist&gt;} [permit {qosprofile &lt;qosprofile&gt;} {set code-point &lt;code_point&gt;} {set dot1p &lt;dot1p_value&gt;}   permit-established   deny] </pre>	<p>Creates an access list. The list is applied to all ingress packets. Options include:</p> <ul style="list-style-type: none"> <li>• <b>&lt;name&gt;</b> — Specifies the access control list name. The access list name can be between 1 and 31 characters.</li> <li>• <b>access-mask</b> — Specifies the associated access mask. Any field specified in the access mask must have a corresponding value specified in the access list.</li> <li>• <b>dest-mac</b> — Specifies the destination MAC address.</li> <li>• <b>source-mac</b> — Specifies the source MAC address.</li> <li>• <b>vlan</b> — Specifies the VLANid.</li> <li>• <b>ethertype</b> — Specify IP, ARP, or the hex value to match.</li> <li>• <b>tos</b> — Specifies the IP precedence value.</li> <li>• <b>code-point</b> — Specifies the DiffServ code point value.</li> <li>• <b>ipprotocol</b> — Specify an IP protocol, or the protocol number</li> <li>• <b>dest-ip</b> — Specifies an IP destination address and subnet mask. A mask length of 32 indicates a host entry.</li> <li>• <b>dest-L4port</b> — Specify the destination port.</li> <li>• <b>source-ip</b> — Specifies an IP source address and subnet mask.</li> <li>• <b>source-L4port</b> — Specify the source port.</li> <li>• <b>icmp-type</b> — Specify the ICMP type.</li> <li>• <b>icmp-code</b> — Specify the ICMP code.</li> <li>• <b>egressport</b> — Specify the egress port</li> <li>• <b>ports</b> — Specifies the ingress port(s) on which this rule is applied.</li> <li>• <b>permit</b> — Specifies the packets that match the access list description are permitted to be forward by this switch. An optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.</li> <li>• <b>set</b> — Modify the DiffServ code point and/or the 802.1p value for matching packets.</li> <li>• <b>permit-established</b> — Specifies a uni-directional session establishment is denied.</li> <li>• <b>deny</b> — Specifies the packets that match the access list description are filtered (dropped) by the switch.</li> </ul>

**Table 39:** Access Control List Configuration Commands (continued)

Command	Description
<pre>create access-mask &lt;access-mask name&gt; {dest-mac} {source-mac} {vlan } {ethertype} {tos   code-point} {ipprotocol} {dest-ip /&lt;mask length&gt;} {dest-L4port} {source-ip /&lt;mask length&gt;} {source-L4port   {icmp-type} {icmp-code}} {permit-established} {egressport} {ports} {precedence &lt;number&gt;}</pre>	<p>Creates an access mask. The mask specifies which packet fields to examine. Options include:</p> <ul style="list-style-type: none"> <li>• <code>&lt;access-mask name&gt;</code> — Specifies the access mask name. The access mask name can be between 1 and 31 characters.</li> <li>• <code>dest-mac</code> — Specifies the destination MAC address field.</li> <li>• <code>source-mac</code> — Specifies the source MAC address field.</li> <li>• <code>vlan</code> — Specifies the VLANid field.</li> <li>• <code>ethertype</code> — Specifies the Ethertype field.</li> <li>• <code>tos</code> — Specifies the IP precedence field.</li> <li>• <code>code-point</code> — Specifies the DiffServ code point field.</li> <li>• <code>ipprotocol</code> — Specifies the IP protocol field.</li> <li>• <code>dest-ip</code> — Specifies the IP destination field and subnet mask. You must supply the subnet mask.</li> <li>• <code>dest-L4port</code> — Specifies the destination port field.</li> <li>• <code>source-ip</code> — Specifies the IP source address field and subnet mask. You must supply the subnet mask.</li> <li>• <code>source-L4port</code> — Specifies the source port field.</li> <li>• <code>icmp-type</code> — Specify the ICMP type field.</li> <li>• <code>icmp-code</code> — Specify the ICMP code field.</li> <li>• <code>permit-established</code> — Specifies the TCP SYN/ACK bit fields.</li> <li>• <code>egressport</code> — Specify the egress port</li> <li>• <code>ports</code> — Specifies the ingress port(s) on which this rule is applied.</li> <li>• <code>precedence</code> — Specifies the access mask precedence number. The range is 1 to 25,600.</li> </ul>

**Table 39:** Access Control List Configuration Commands (continued)

Command	Description
<pre> create rate-limit &lt;rule_name&gt; access-mask &lt;access-mask name&gt; {dest-mac &lt;dest_mac&gt;} {source-mac &lt;src_mac&gt;} {vlan &lt;name&gt;} {ethertype [IP   ARP   &lt;hex_value&gt;]} {tos &lt;ip_precedence&gt;   code-point &lt;code_point&gt;} {ipprotocol [tcp udp icmp igmp &lt;protocol_num&gt;]} {dest-ip &lt;dest_IP&gt;/&lt;mask length&gt;} {dest-L4port &lt;dest_port&gt;} {source-ip &lt;src_IP&gt;/&lt;mask length&gt;} {source-L4port &lt;src_port&gt;   {icmp-type &lt;icmp_type&gt;} {icmp-code &lt;icmp_code&gt;}} {egressport &lt;port&gt;} {port &lt;port number&gt;} permit {qosprofile &lt;qosprofile&gt;} {set code-point &lt;code_point&gt;} {set dot1p &lt;dot1p_value&gt;} limit &lt;rate_in_Mbps&gt; {exceed-action [drop   set code-point &lt;code_point&gt;} </pre>	<p>Creates a rate limit. The rule is applied to all ingress packets. Options include:</p> <ul style="list-style-type: none"> <li>• <code>&lt;rule_name&gt;</code> — Specifies the rate limit name. The name can be between 1 and 31 characters.</li> <li>• <code>access-mask</code> — Specifies the associated access mask. Any field specified in the access mask must have a corresponding value specified in the rate limit.</li> <li>• <code>dest-mac</code> — Specifies the destination MAC address.</li> <li>• <code>source-mac</code> — Specifies the source MAC address.</li> <li>• <code>vlan</code> — Specifies the VLANid.</li> <li>• <code>ethertype</code> — Specify IP, ARP, or the hex value to match.</li> <li>• <code>tos</code> — Specifies the IP precedence value.</li> <li>• <code>code-point</code> — Specifies the DiffServ code point value.</li> <li>• <code>ipprotocol</code> — Specify an IP protocol, or the protocol number</li> <li>• <code>dest-ip</code> — Specifies the IP destination address and subnet mask. A mask length of 32 indicates a host entry.</li> <li>• <code>dest-L4port</code> — Specify the destination port.</li> <li>• <code>source-ip</code> — Specifies the IP source address and subnet mask.</li> <li>• <code>source-L4port</code> — Specify the source port.</li> <li>• <code>icmp-type</code> — Specify the ICMP type.</li> <li>• <code>icmp-code</code> — Specify the ICMP code.</li> <li>• <code>egressport</code> — Specify the egress port</li> <li>• <code>port</code> — Specifies the ingress port to which this rule is applied.</li> <li>• <code>permit</code> — Specifies the packets that match the access list description are permitted to be forward by this switch. An optional QoS profile can be assigned to the access list, so that the switch can prioritize packets accordingly.</li> <li>• <code>set</code> — Modify the DiffServ code point or the 802.1p value for matching, forwarded, packets.</li> <li>• <code>limit</code> — Specifies the rate limit</li> <li>• <code>&lt;rate_in_Mbps&gt;</code> — The rate limit. Allowed values are 1-100 Mbps for 100BT ports, 8, 16, 24, 32... 1000 for the Gigabit ports</li> <li>• <code>exceed-action</code> — Action to take for matching packets that exceed the rate.</li> </ul>
<pre> delete access-list &lt;name&gt; </pre>	<p>Deletes an access list.</p>

**Table 39:** Access Control List Configuration Commands (continued)

Command	Description
delete access-mask <name>	Deletes an access mask. Any access lists or rate limits that reference this mask must first be deleted.
delete rate-limit <name>	Deletes a rate limit.
show access-list {<name>   ports <portlist>}	Displays access-list information.
show access-mask {<name>}	Displays access-list information.
show rate-limit {<name>   ports <portlist>}	Displays access-list information.

## Access Control List Examples

This section presents three access control list examples:

- Using the permit-establish keyword
- Filtering ICMP packets
- Using a rate limit

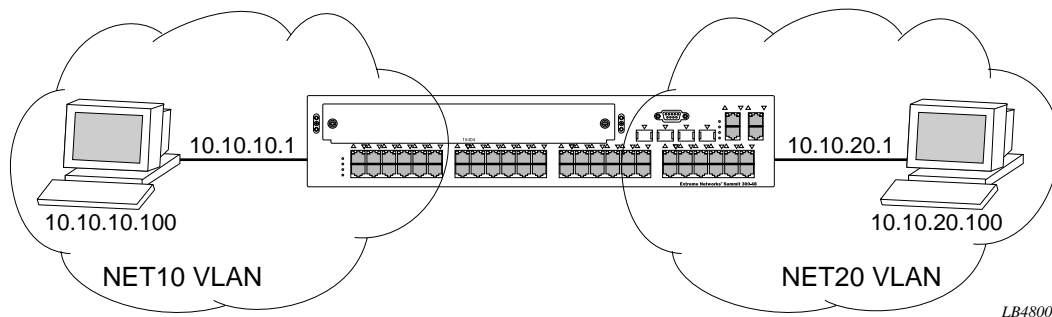
### Using the Permit-Established Keyword

This example uses an access list that permits TCP sessions (Telnet, FTP, and HTTP) to be established in one direction.

The switch, shown in Figure 7, is configured as follows:

- Two VLANs, NET10 VLAN and NET20 VLAN, are defined.
- The NET10 VLAN is connected to port 1:2 and the NET20 VLAN is connected to port 1:10
- The IP addresses for NET10 VLAN is 10.10.10.1/24.
- The IP address for NET20 VLAN is 10.10.20.1/24.
- The workstations are configured using addresses 10.10.10.100 and 10.10.20.100.
- IPForwarding is enabled.

**Figure 7:** Permit-established access list example topology



LB48009

The following sections describe the steps used to configure the example.

### Step 1 – Deny IP Traffic.

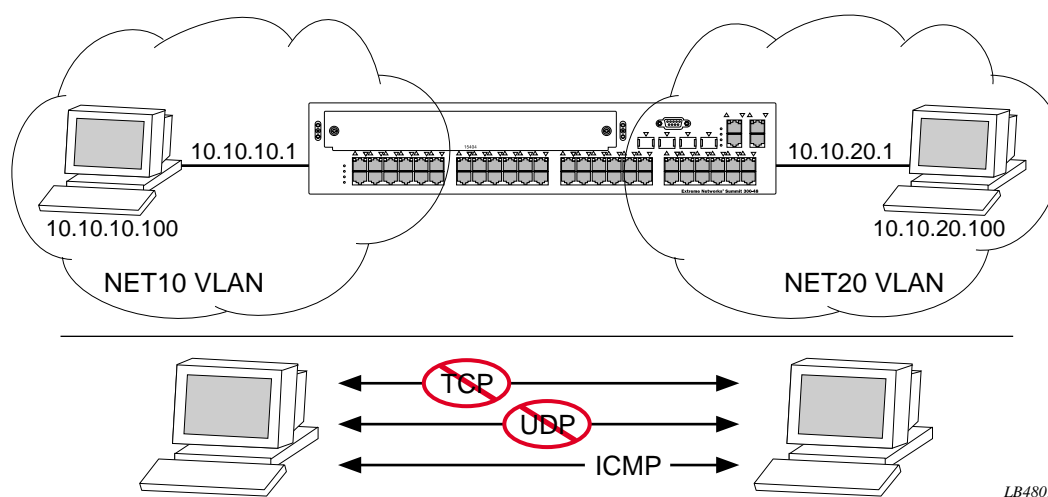
First, create an access-mask that examines the IP protocol field for each packet. Then create two access-lists, one that blocks all TCP, one that blocks UDP. Although ICMP is used in conjunction with IP, it is technically not an IP data packet. Thus, ICMP data traffic, such as ping traffic, is not affected.

The following commands create the access mask and access lists:

```
create access-mask ipproto_mask ipprotocol ports precedence 25000
create access-list denytcp ipproto_mask ipprotocol tcp ports 1:2,1:10 deny
create access-list denyudp ipproto_mask ipprotocol udp ports 1:2,1:10 deny
```

Figure 8 illustrates the outcome of the access control list.

**Figure 8:** Access control list denies all TCP and UDP traffic



### Step 2 – Allow TCP traffic.

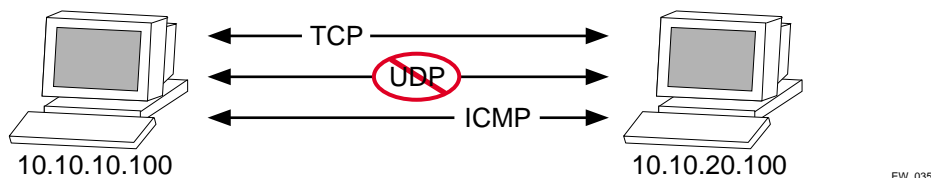
The next set of access list commands permits TCP-based traffic to flow. Because each session is bi-directional, an access list must be defined for each direction of the traffic flow. UDP traffic is still blocked.

The following commands create the access control list:

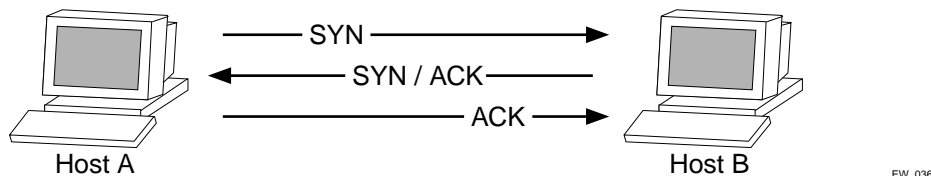
```
create access-mask ip_addr_mask ipprotocol dest-ip/32 source-ip/32 ports precedence
20000

create access-list tcp1_2 ip_addr_mask ipprotocol tcp dest-ip 10.10.20.100/32
source-ip 10.10.10.100/32 ports 1:2 permit qpl
create access-list tcp2_1 ip_addr_mask ipprotocol tcp dest-ip 10.10.10.100/32
source-ip 10.10.20.100/32 ports 1:10 permit qpl
```

Figure 9 illustrates the outcome of this access list.

**Figure 9:** Access list allows TCP traffic**Step 3 - Permit-Established Access List.**

When a TCP session begins, there is a three-way handshake that includes a sequence of a SYN, SYN/ACK, and ACK packets. Figure 10 shows an illustration of the handshake that occurs when host A initiates a TCP session to host B. After this sequence, actual data can be passed.

**Figure 10:** Host A initiates a TCP session to host B

An access list that uses the permit-established keyword filters the SYN packet in one direction.

Use the permit-established keyword to allow only host A to be able to establish a TCP session to host B and to prevent any TCP sessions from being initiated by host B, as illustrated in Figure 10. The commands for this access control list is as follows:

```
create access-mask tcp_connection_mask ipprotocol dest-ip/32 dest-L4port
  permit-established ports precedence 1000
create access-list telnet-deny tcp_connection_mask ipprotocol tcp dest-ip
  10.10.10.100/32 dest-L4port 23 ports 1:10 permit-established
```

**NOTE**

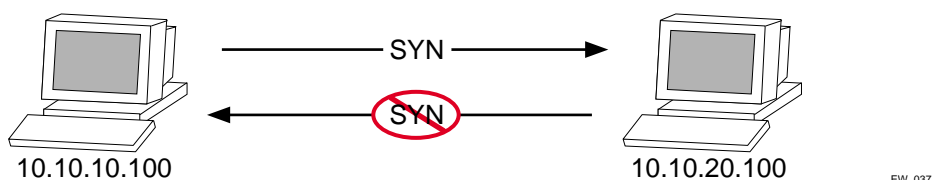
*This step may not be intuitive. Pay attention to the destination and source address, the ingress port that the rule is applied to, and the desired affect.*

**NOTE**

*This rule has a higher precedence than the rule "tcp2\_1" and "tcp1\_2".*

Figure 11 shows the final outcome of this access list.

**Figure 11:** Permit-established access list filters out SYN packet to destination



### Example 2: Filter ICMP Packets

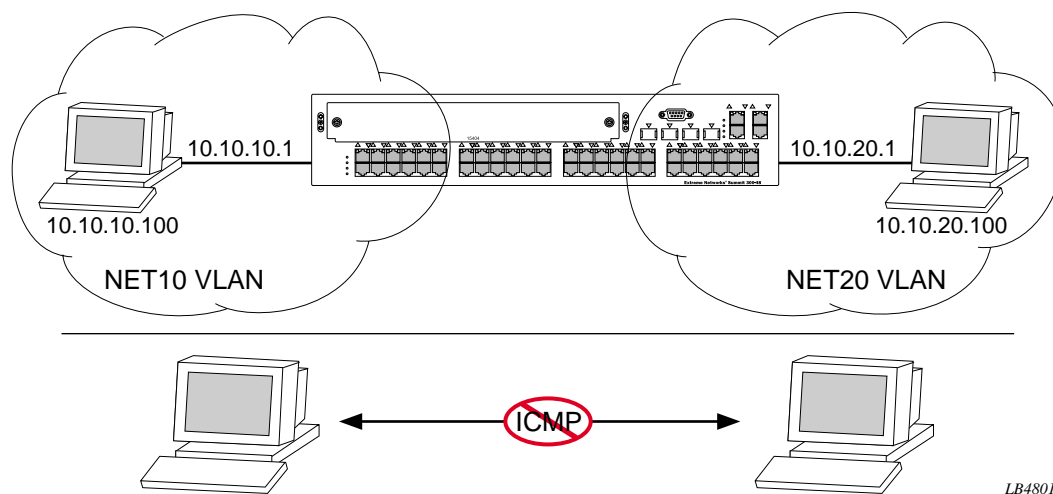
This example creates an access list that filters out ping (ICMP echo) packets. ICMP echo packets are defined as type 8 code 0.

The commands to create this access control list is as follows:

```
create access-mask icmp_mask ipprotocol icmp-type icmp-code
create access-list denyicmp icmp_mask ipprotocol icmp icmp-type 8 icmp-code 0 deny
```

The output for this access list is shown in Figure 12.

**Figure 12:** ICMP packets are filtered out



### Example 3: Rate-limiting Packets

This example creates a rate limit to limit the incoming traffic from the 10.10.10.x subnet to 10 Mbps on ingress port 2. Ingress traffic on port 2 below the rate limit is sent to QoS profile *qp1* with its DiffServ code point set to 7. Ingress traffic on port 2 in excess of the rate limit will be dropped.

The commands to create this rate limit is as follows:

```
create access-mask port2_mask source-ip/24 ports precedence 100
create rate-limit port2_limit port2_mask source-ip 10.10.10.0/24 ports 1:2 permit qp1
set code-point 7 limit 10 exceed-action drop
```





# 11

## Quality of Service (QoS)

---

This chapter describes the following topics:

- Overview of Policy-Based Quality of Service on page 121
- Applications and Types of QoS on page 122
- Configuring QoS for a Port or VLAN on page 123
- Traffic Groupings on page 124
  - MAC-Based Traffic Groupings on page 125
  - Explicit Class of Service (802.1p and DiffServ) Traffic Groupings on page 126
  - Physical and Logical Groupings on page 130
- Verifying Configuration and Performance on page 131
- Modifying a QoS Configuration on page 132
- Traffic Rate-Limiting on page 132

Policy-based Quality of Service (QoS) is a feature of ExtremeWare and the Extreme switch architecture that allows you to specify different service levels for traffic traversing the switch. Policy-based QoS is an effective control mechanism for networks that have heterogeneous traffic patterns. Using Policy-based QoS, you can specify the service level that a particular traffic type receives.

### Overview of Policy-Based Quality of Service

Policy-based QoS allows you to protect bandwidth for important categories of applications or specifically limit the bandwidth associated with less critical traffic. For example, if voice-over-IP traffic requires a reserved amount of bandwidth to function properly, using QoS, you can reserve sufficient bandwidth critical to this type of application. Other applications deemed less critical can be limited so as to not consume excessive bandwidth. The switch contains separate hardware queues on every physical port. Each hardware queue can be programmed by ExtremeWare with bandwidth limitation and prioritization parameters. The bandwidth limitation and prioritization parameters that modify the forwarding behavior of the switch affect how the switch transmits traffic for a given hardware queue on a physical port.

Summit 300-48 switches support up to four physical queues per port.



---

*As with all Extreme switch products, QoS has no impact on switch performance. Using even the most complex traffic groupings has no cost in terms of switch performance.*

## Applications and Types of QoS

Different applications have different QoS requirements. The following applications are ones that you will most commonly encounter and need to prioritize:

- Voice applications
- Video applications
- Critical database applications
- Web browsing applications
- File server applications

General guidelines for each traffic type are given below and summarized in Table 40. Consider them as general guidelines and not strict recommendations. Once QoS parameters are set, you can monitor the performance of the application to determine if the actual behavior of the applications matches your expectations. It is very important to understand the needs and behavior of the particular applications you wish to protect or limit. Behavioral aspects to consider include bandwidth needs, sensitivity to latency and jitter, and sensitivity and impact of packet loss.

### Voice Applications

Voice applications typically demand small amounts of bandwidth. However, the bandwidth must be constant and predictable because voice applications are typically sensitive to latency (inter-packet delay) and jitter (variation in inter-packet delay). The most important QoS parameter to establish for voice applications is minimum bandwidth, followed by priority.

### Video Applications

Video applications are similar in needs to voice applications, with the exception that bandwidth requirements are somewhat larger, depending on the encoding. It is important to understand the behavior of the video application being used. For example, in the playback of stored video streams, some applications can transmit large amounts of data for multiple streams in one “spike,” with the expectation that the end-stations will buffer significant amounts of video-stream data. This can present a problem to the network infrastructure, because it must be capable of buffering the transmitted spikes where there are speed differences (for example, going from Gigabit Ethernet to Fast Ethernet). Key QoS parameters for video applications include minimum bandwidth, priority, and possibly buffering (depending upon the behavior of the application).

### Critical Database Applications

Database applications, such as those associated with ERP, typically do not demand significant bandwidth and are tolerant of delay. You can establish a minimum bandwidth using a priority less than that of delay-sensitive applications.

## Web Browsing Applications

QoS needs for Web browsing applications cannot be generalized into a single category. For example, ERP applications that use a browser front-end may be more important than retrieving daily news information. Traffic groupings can typically be distinguished from each other by their server source and destinations. Most browser-based applications are distinguished by the dataflow being asymmetric (small dataflows from the browser client, large dataflows from the server to the browser client).

An exception to this may be created by some Java™ -based applications. In addition, Web-based applications are generally tolerant of latency, jitter, and some packet loss, however small packet-loss may have a large impact on perceived performance due to the nature of TCP. The relevant parameter for protecting browser applications is minimum bandwidth. The relevant parameter for preventing non-critical browser applications from overwhelming the network is maximum bandwidth. In addition, RED can be used to reduce session loss if the queue that floods Web traffic becomes over-subscribed.

## File Server Applications

With some dependencies on the network operating system, file serving typically poses the greatest demand on bandwidth, although file server applications are very tolerant of latency, jitter, and some packet loss, depending on the network operating system and the use of TCP or UDP.



### NOTE

*Full-duplex links should be used when deploying policy-based QoS. Half-duplex operation on links can make delivery of guaranteed minimum bandwidth impossible.*

Table 40 summarizes QoS guidelines for the different types of network traffic.

**Table 40:** Traffic Type and QoS Guidelines

Traffic Type	Key QoS Parameters
Voice	Minimum bandwidth, priority
Video	Minimum bandwidth, priority, buffering (varies)
Database	Minimum bandwidth
Web browsing	Minimum bandwidth for critical applications, maximum bandwidth for non-critical applications, RED
File server	Minimum bandwidth

## Configuring QoS for a Port or VLAN

Table 41 lists the commands used to configure QoS.

**Table 41:** QoS Configuration Commands

Command	Description
config ports <portlist> qosprofile <qosprofile>	Configures one or more ports to use a particular QoS profile.
config vlan <name> qosprofile <qosprofile>	Allows you to configure a VLAN to use a particular QoS profile.

## Traffic Groupings

After a QoS profile has been modified for bandwidth and priority, you assign traffic a grouping to the profile. A *traffic grouping* is a classification of traffic that has one or more attributes in common. Traffic is typically grouped based on the applications discussed starting on page -122.

Traffic groupings are separated into the following categories for discussion:

- Access list based information, such as IP source/destination, TCP/UDP port information, and VLANid
- Destination MAC (MAC QoS groupings)
- Explicit packet class of service information, such as 802.1p or DiffServ (IP TOS)
- Physical/logical configuration (physical source port or VLAN association)

In the event that a given packet matches two or more grouping criteria, there is a predetermined precedence for which traffic grouping will apply. In general, the more specific traffic grouping takes precedence. By default, all traffic groupings are placed in the QoS profile Qp1. The supported traffic groupings are listed in Table 42. The groupings are listed in order of precedence (highest to lowest). The four types of traffic groupings are described in detail on the following pages.

**Table 42:** Traffic Groupings by Precedence

---

### IP Information (Access Lists) Grouping

- Access list precedence determined by user configuration

---

### Explicit Packet Class of Service Groupings

- DiffServ (IP TOS)
- 802.1P

---

### Destination Address MAC-Based Groupings

- Permanent
- Dynamic
- Blackhole

---

### Physical/Logical Groupings

- Source port
  - VLAN
- 

## Access List Based Traffic Groupings

Access list based traffic groupings are based on any combination of the following items:

- IP source or destination address
- TCP/UDP or other layer 4 protocol
- TCP/UDP port information
- MAC source or destination address
- VLANid

Access list based traffic groupings are defined using access lists. Access lists are discussed in detail in Chapter 10. By supplying a named QoS profile at the end of the access list command syntax, you can

prescribe the bandwidth management and priority handling for that traffic grouping. This level of packet filtering has no impact on performance.

## MAC-Based Traffic Groupings

QoS profiles can be assigned to destination MAC addresses. MAC-based traffic groupings are configured using the following command:

```
create fdbentry <mac_address> vlan <name> [blackhole | port <portlist> | dynamic]
qosprofile <qosprofile>
```

The MAC address options, defined below, are as follows:

- Permanent
- Dynamic
- Blackhole

### Permanent MAC addresses

Permanent MAC addresses can be assigned a QoS profile whenever traffic is destined to the MAC address. This can be done when you create a permanent FDB entry. For example:

```
create fdbentry 00:11:22:33:44:55 vlan default port 1:4 qosprofile qp2
```

### Dynamic MAC Addresses

Dynamic MAC addresses can be assigned a QoS profile whenever traffic is destined to the MAC address. For any port on which the specified MAC address is learned in the specified VLAN, the port is assigned the specified QoS profile. For example:

```
create fdbentry 00:11:22:33:44:55 vlan default dynamic qosprofile qp3
```

The QoS profile is assigned when the MAC address is learned. If a client's location moves, the assigned QoS profile moves with the device. If the MAC address entry already exists in the FDB, you can clear the forwarding database so that the QoS profile can be applied when the entry is added again. Use the following command to clear the FDB:

```
clear fdb
```

### Blackhole MAC Address

Using the `blackhole` option configures the switch to not forward any packets to the destination MAC address on any ports for the VLAN specified. The `blackhole` option is configured using the following command:

```
create fdbentry 00:11:22:33:44:55 vlan default blackhole
```

### Verifying MAC-Based QoS Settings

To verify any of the MAC-based QoS settings, use either the command

```
show fdb permanent
```

or the command

```
show qosprofile <qosprofile>
```

## Explicit Class of Service (802.1p and DiffServ) Traffic Groupings

This category of traffic groupings describes what is sometimes referred to as *explicit packet marking*, and refers to information contained within a packet intended to explicitly determine a class of service. That information includes:

- IP DiffServ code points, formerly known as IP TOS bits
- Prioritization bits used in IEEE 802.1p packets

An advantage of explicit packet marking is that the class of service information can be carried throughout the network infrastructure, without repeating what can be complex traffic grouping policies at each switch location. Another advantage is that end stations can perform their own packet marking on an application-specific basis. The Summit 300-48 switch has the capability of observing and manipulating packet marking information with no performance penalty.

The documented capabilities for 802.1p priority markings or DiffServ capabilities are not impacted by the switching or routing configuration of the switch. For example, 802.1p information can be preserved across a routed switch boundary and DiffServ code points can be observed or overwritten across a layer 2 switch boundary.



### NOTE

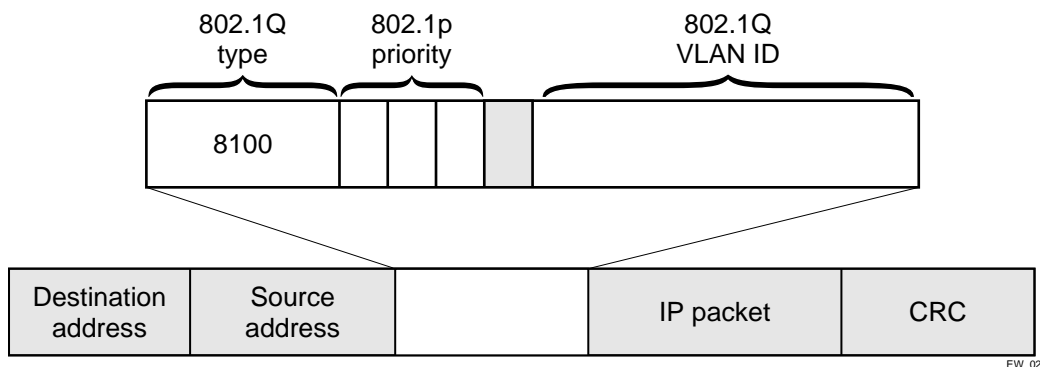
*Re-marking DiffServ code points is supported through access lists. See Chapter 10, “Access Policies”, for more information.*

### Configuring 802.1p Priority

Extreme switches support the standard 802.1p priority bits that are part of a tagged Ethernet packet. The 802.1p bits can be used to prioritize the packet, and assign it to a particular QoS profile.

When a packet arrives at the switch, the switch examines the 802.1p priority field maps it to a specific hardware queue when subsequently transmitting the packet. The 802.1p priority field is located directly following the 802.1Q type field, and preceding the 802.1Q VLAN ID, as shown in Figure 13.

**Figure 13:** Ethernet packet encapsulation



### Observing 802.1p Information

When ingress traffic that contains 802.1p prioritization information is detected by the switch, the traffic is mapped to various hardware queues on the egress port of the switch. The Summit 300-48 switch

supports four hardware queues. The transmitting hardware queue determines the bandwidth management and priority characteristics used when transmitting packets.

To control the mapping of 802.1p prioritization values to hardware queues, 802.1p prioritization values can be mapped to a QoS profile. The default mapping of each 802.1p priority value to QoS profile is shown in Table 43.

**Table 43:** 802.1p Priority Value-to-QoS Profile to Hardware Queue Default Mapping

Priority Value	QoS Profile	Hardware Queue Priority Value
0	Qp1	1
1	Qp2	1
2	Qp3	2
3	Qp4	2
4	Qp5	3
5	Qp6	3
6	Qp7	4
7	Qp8	4

## 802.1p Commands

Table 44 shows the command used to configure 802.1p priority. This is explained in more detail in the following paragraphs.

**Table 44:** 802.1p Configuration Commands

Command	Description
<code>config vlan &lt;name&gt; priority &lt;number&gt;</code>	Configures the 802.1p priority value for 802.1Q VLAN tags. The value for <code>priority</code> is an integer between 0 and 7.

## Configuring 802.1p Priority

When a packet is transmitted by the switch, you can configure the 802.1p priority field that is placed in the 802.1Q tag. You can configure the priority to be a number between 0 and 7, using the following command:

```
config vlan <name> priority <number>
```

## Replacing 802.1p Priority Information

By default, 802.1p priority information is not replaced or manipulated, and the information observed on ingress is preserved when transmitting the packet. This behavior is not affected by the switching or routing configuration of the switch.

However, the switch is capable of replacing the 802.1p priority information. To replace 802.1p priority information, you will use an access list to set the 802.1p value. See Chapter 10, “Access Policies”, for more information on using access lists. You will use the `set dot1p <dot1p_value>` parameter of the `create access list` command to replace the value. The packet is then placed on the queue that corresponds to the new 802.1p value.

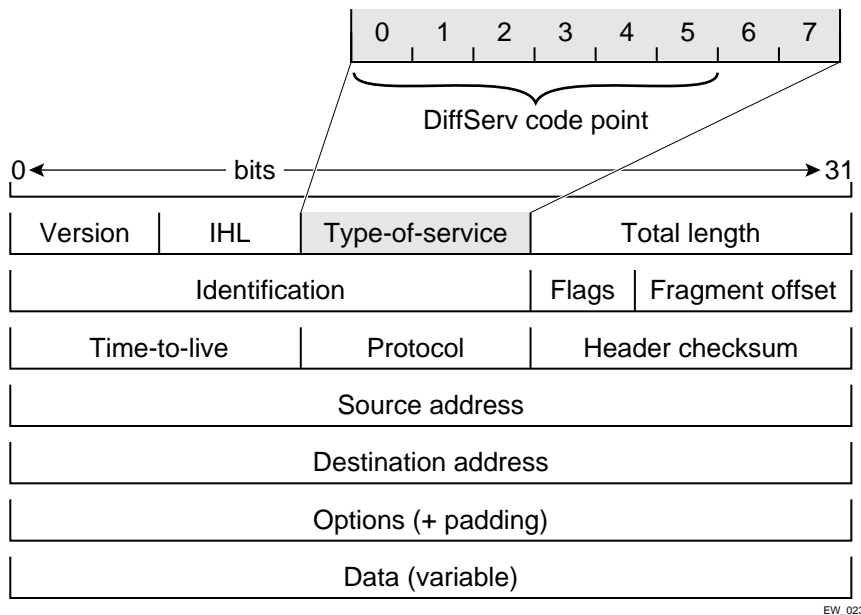
## Configuring DiffServ

Contained in the header of every IP packet is a field for IP Type of Service (TOS), now also called the DiffServ field. The TOS field is used by the switch to determine the type of service provided to the packet.

Observing DiffServ code points as a traffic grouping mechanism for defining QoS policies and overwriting the Diffserv code point fields are supported in the Summit 300-48 switch.

Figure 14 shows the encapsulation of an IP packet header.

**Figure 14:** IP packet header encapsulation



EW\_023

Table 45 lists the commands used to configure DiffServ. Some of the commands are described in more detail in the following paragraphs.

**Table 45:** DiffServ Configuration Commands

Command	Description
disable diffserv examination ports [<portlist>   all]	Disables the examination of the diffserv field in an IP packet.
enable diffserv examination ports [<portlist>   all]	Enables the diffserv field of an ingress IP packet to be examined by the switch in order to select a QoS profile. The default setting is disabled.



## Observing DiffServ Information

When a packet arrives at the switch on an ingress port, the switch examines the first six of eight TOS bits, called the *code point*. The switch can assign the QoS profile used to subsequently transmit the packet based on the code point. The QoS profile controls a hardware queue used when transmitting the packet out of the switch, and determines the forwarding characteristics of a particular code point. Viewing DiffServ information can be enabled or disabled; by default it is disabled. To view DiffServ information, use the following command:

```
enable diffserv examination ports [<portlist> | all]
```



### NOTE

*DiffServ examination requires one access mask while it is enabled. See “Maximum Entries” on page 111 for more information.*

## Changing DiffServ Code point assignments in the QoS Profile

The DiffServ code point has 64 possible values ( $2^6 = 64$ ). By default, the values are grouped and assigned to the default QoS profiles listed in Table 46.

**Table 46:** Default Code Point-to-QoS Profile Mapping

Code Point	QoS Profile
0-7	Qp1
8-15	Qp2
16-23	Qp3
24-31	Qp4
32-39	Qp5
40-47	Qp6
48-55	Qp7
56-63	Qp8

You can change the QoS profile assignment for a code point by using an access list. See Chapter 10, “Access Policies”, for more information.

## Replacing DiffServ Code Points

An access list can be used to change the DiffServ code point in the packet prior to the packet being transmitted by the switch. This is done with no impact on switch performance.

To replace the DiffServ code point, you will use an access list to set the new code point value. See Chapter 10, “Access Policies”, for more information on using access lists. You will use the `set code-point` parameter of the `create access list` command to replace the value.

To display the DiffServ configuration, use the following command:

```
show ports <portlist> info {detail}
```



### NOTE

*The show ports command displays only the default code point mapping.*

## DiffServ Examples

For information on the access list and access mask commands in the following examples, see Chapter 10, “Access Policies”.

Use the following command to use the DiffServe code point value to assign traffic to the hardware queues:

```
enable diffserv examination ports all
```

In the following example, all the traffic from network 10.1.2.x is assigned the DiffServe code point 23 and the 802.1p value of 2:

```
create access-mask SrcIpMask source-ip/24
create access-list TenOneTwo access-mask SrcIpMask source-ip 10.1.2.0/24 permit qp3
    set code-point 23 set dot1p 2
```

## Physical and Logical Groupings

Two traffic groupings exist in this category:

- Source port
- VLAN

### Source port

A source port traffic grouping implies that any traffic sourced from this physical port uses the indicated QoS profile when the traffic is transmitted out to any other port. To configure a source port traffic grouping, use the following command:

```
config ports <portlist> qosprofile <qosprofile>
```

In the following modular switch example, all traffic sourced from port 7 uses the QoS profile named *qp3* when being transmitted.

```
config ports 7 qosprofile qp3
```

### VLAN

A VLAN traffic grouping indicates that all intra-VLAN switched traffic and all routed traffic sourced from the named VLAN uses the indicated QoS profile. To configure a VLAN traffic grouping, use the following command:

```
config vlan <name> qosprofile <qosprofile>
```

For example, all devices on VLAN *servnet* require use of the QoS profile *qp4*. The command to configure this example is as follows:

```
config vlan servnet qosprofile qp4
```

## Verifying Physical and Logical Groupings

To verify settings on ports or VLANs, use the following command:

```
show qosprofile <qosprofile>
```

The same information is also available for ports or VLANs using one of the following commands:

```
show ports <portlist> info {detail}
```

or

```
show vlan
```

## Verifying Configuration and Performance

After you have created QoS policies that manage the traffic through the switch, you can use the QoS monitor to determine whether the application performance meets your expectations.

### QoS Monitor

The QoS monitor is a utility that monitors the incoming packets on a port or ports. The QoS monitor keeps track of the number of frames and the frames per second, sorted by 802.1p value, on each monitored port.

### Real-Time Performance Monitoring

The real-time display scrolls through the given portlist to provide statistics. You can choose screens for packet count and packets per second.

To view real-time switch per-port performance, use the following command:

```
show ports {<portlist>} qosmonitor
```

The QoS monitor rate screen (packets per second), does not display any results for at least five seconds. After the rate has been displayed, it is updated each second.



#### NOTE

---

*The QoS monitor can display up to four ports at a time.*



#### NOTE

---

*The QoS monitor displays the statistics of incoming packets. The real-time display corresponds to the 802.1p values of the incoming packets. Any priority changes within the switch are not reflected in the display.*



#### NOTE

---

*The QoS monitor requires one access mask until it exits. See “Maximum Entries” on page 111 for more information.*

## Displaying QoS Profile Information

The QoS monitor can also be used to verify the QoS configuration and monitor the use of the QoS policies that are in place. To display QoS information on the switch, use the following command:

```
show qosprofile <qosprofile>
```

Displayed information includes:

- QoS profile name
- Minimum bandwidth
- Maximum bandwidth
- Priority
- A list of all traffic groups to which the QoS profile is applied

Additionally, QoS information can be displayed from the traffic grouping perspective by using one or more of the following commands:

- `show fdb permanent` — Displays destination MAC entries and their QoS profiles.
- `show switch` — Displays information including PACE enable/disable information.
- `show vlan` — Displays the QoS profile assignments to the VLAN.
- `show ports <portlist> info {detail}` — Displays information including QoS information for the port.

## Modifying a QoS Configuration

If you make a change to the parameters of a QoS profile after implementing your configuration, the timing of the configuration change depends on the traffic grouping involved. The following rules apply:

- For destination MAC-based grouping (other than permanent), clear the MAC FDB using the command `clear fdb`. This command should also be issued after a configuration is implemented, as the configuration must be in place before an entry is made in the MAC FDB. For permanent destination MAC-based grouping, re-apply the QoS profile to the static FDB entry, as documented. You can also save and reboot the switch.
- For physical and logical groupings of a source port or VLAN, re-apply the QoS profile to the source port or VLAN, as documented. You can also save and reboot the switch.

## Traffic Rate-Limiting

The Summit 300-48 rate-limiting method is based on creating a rate limit, a specific type of access control list. Traffic that matches a rate limit is constrained to the limit set in the access control list. Rate limits are discussed in Chapter 10, “Access Policies”.

# 12

## Status Monitoring and Statistics

---

This chapter describes the following topics:

- Status Monitoring on page 133
- Port Statistics on page 135
- Port Errors on page 136
- Port Monitoring Display Keys on page 137
- Setting the System Recovery Level on page 137
- Logging on page 138
- RMON on page 142

Viewing statistics on a regular basis allows you to see how well your network is performing. If you keep simple daily records, you will see trends emerging and notice problems arising before they cause major network faults. In this way, statistics can help you get the best out of your network.

### Status Monitoring

The status monitoring facility provides information about the switch. This information may be useful for your technical support representative if you have a problem. ExtremeWare includes many show commands that display information about different switch functions and facilities.



---

*For more information about show commands for a specific ExtremeWare feature, see the appropriate chapter in this guide.*

Table 47 describes commands that are used to monitor the status of the switch.

**Table 47: Status Monitoring Commands**

Command	Description
show log {<priority>}	Displays the current snapshot of the log. Options include: <ul style="list-style-type: none"> <li>• <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, all messages are displayed.</li> </ul>
show log config	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.
show memory {detail}	Displays the current system memory information. Specify the <code>detail</code> option to view task-specific memory usage.
show switch	Displays the current switch information, including: <ul style="list-style-type: none"> <li>• <code>sysName</code>, <code>sysLocation</code>, <code>sysContact</code></li> <li>• MAC address</li> <li>• License</li> <li>• System mode</li> <li>• Recovery mode</li> <li>• DLCS status</li> <li>• Current time, timezone and boot time</li> <li>• Scheduled reboot information</li> <li>• Timed upload, download</li> <li>• Temperature, fan, and power supply status</li> <li>• Eware image, config, bootloader, and bootstrap information including versions currently stored in the switch</li> </ul>

**Table 47:** Status Monitoring Commands (continued)

Command	Description
show tech-support	<p>Displays the output for the following commands:</p> <ul style="list-style-type: none"> <li>• show version</li> <li>• show switch</li> <li>• show config</li> <li>• show diag</li> <li>• show gdb</li> <li>• show iparp</li> <li>• show ipfdb</li> <li>• show ipstats</li> <li>• show iproute</li> <li>• show ipmc cache detail</li> <li>• show igmp snooping detail</li> <li>• show memory detail</li> <li>• show log</li> </ul> <p>It also displays the output from internal debug commands. This command disables the CLI paging feature.</p>
show version	Displays the hardware and software versions currently running on the switch.

## Port Statistics

ExtremeWare provides a facility for viewing port statistic information. The summary information lists values for the current counter against each port on each operational module in the system, and it is refreshed approximately every 2 seconds. Values are displayed to nine digits of accuracy.

To view port statistics, use the following command:

```
show ports <portlist> stats
```

The following port statistic information is collected by the switch:

- **Link Status** — The current status of the link. Options are:
  - Ready (the port is ready to accept a link).
  - Active (the link is present at this port).
  - Chassis (the link is connected to a Summit Virtual Chassis).
- **Transmitted Packet Count (Tx Pkt Count)** — The number of packets that have been successfully transmitted by the port.
- **Transmitted Byte Count (Tx Byte Count)** — The total number of data bytes successfully transmitted by the port.
- **Received Packet Count (Rx Pkt Count)** — The total number of good packets that have been received by the port.

- **Received Byte Count (RX Byte Count)** — The total number of bytes that were received by the port, including bad or lost frames. This number includes bytes contained in the Frame Check Sequence (FCS), but excludes bytes in the preamble.
- **Received Broadcast (RX Bcast)** — The total number of frames received by the port that are addressed to a broadcast address.
- **Received Multicast (RX Mcast)** — The total number of frames received by the port that are addressed to a multicast address.

## Port Errors

The switch keeps track of errors for each port.

To view port transmit errors, use the following command:

```
show ports <portlist> txerrors
```

The following port transmit error information is collected by the system:

- **Port Number**
- **Link Status** — The current status of the link. Options are:
  - Ready (the port is ready to accept a link).
  - Active (the link is present at this port).
- **Transmit Collisions (TX Coll)** — The total number of collisions seen by the port, regardless of whether a device connected to the port participated in any of the collisions.
- **Transmit Late Collisions (TX Late Coll)** — The total number of collisions that have occurred after the port's transmit window has expired.
- **Transmit Deferred Frames (TX Deferred)** — The total number of frames that were transmitted by the port after the first transmission attempt was deferred by other network traffic.
- **Transmit Errored Frames (TX Error)** — The total number of frames that were not completely transmitted by the port because of network errors (such as late collisions or excessive collisions).
- **Transmit Parity Frames (TX Parity)** — The bit summation has a parity mismatch.

To view port receive errors, use the following command:

```
show ports <portlist> rxerrors
```

The following port receive error information is collected by the switch:

- **Link Status** — The current status of the link. Options are:
  - Ready (the port is ready to accept a link).
  - Active (the link is present at this port).
- **Receive Bad CRC Frames (RX CRC)** — The total number of frames received by the port that were of the correct length, but contained a bad FCS value.
- **Receive Oversize Frames (RX Over)** — The total number of good frames received by the port greater than the supported maximum length of 1,522 bytes.
- **Receive Undersize Frames (RX Under)** — The total number of frames received by the port that were less than 64 bytes long.



- **Receive Fragmented Frames (RX Frag)** — The total number of frames received by the port were of incorrect length and contained a bad FCS value.
- **Receive Jabber Frames (RX Jab)** — The total number of frames received by the port that was of greater than the support maximum length and had a Cyclic Redundancy Check (CRC) error.
- **Receive Alignment Errors (RX Align)** — The total number of frames received by the port that occurs if a frame has a CRC error and does not contain an integral number of octets.
- **Receive Frames Lost (RX Lost)** — The total number of frames received by the port that were lost because of buffer overflow in the switch.

## Port Monitoring Display Keys

Table 48 describes the keys used to control the displays that appear when you issue any of the `show port` commands.

**Table 48:** Port Monitoring Display Keys

Key(s)	Description
U	Displays the previous page of ports.
D	Displays the next page of ports.
[Esc] or [Return]	Exits from the screen.
0	Clears all counters.
[Space]	Cycles through the following screens: <ul style="list-style-type: none"> <li>• Packets per second</li> <li>• Bytes per second</li> <li>• Percentage of bandwidth</li> </ul> <p>Available using the <code>show port utilization</code> command only.</p>

## Setting the System Recovery Level

You can configure the system to automatically reboot after a software task exception, using the following command:

```
config sys-recovery-level [none | critical | all]
```

Where the following is true:

- `none` — Configures the level to recovery without a system reboot.
- `critical` — Configures ExtremeWare to log an error into the syslog and automatically reboot the system after a critical exception.
- `all` — Configures ExtremeWare to log an error into the syslog and automatically reboot the system after any exception.

The default setting is `none`.

**NOTE**

*Extreme Networks recommends that you set the system recovery level to `critical`. This allows ExtremeWare to log an error to the syslog and automatically reboot the system after a critical exception.*

## Logging

The switch log tracks all configuration and fault information pertaining to the device. Each entry in the log contains the following information:

- **Timestamp** — The timestamp records the month and day of the event, along with the time (hours, minutes, and seconds) in the form HH:MM:SS. If the event was caused by a user, the user name is also provided.
- **Fault level** — Table 49 describes the four levels of importance that the system can assign to a fault.

**Table 49:** Fault Levels Assigned by the Switch

Level	Description
Critical	A desired switch function is inoperable. The switch may need to be reset.
Warning	A noncritical error that may lead to a function failure.
Informational	Actions and events that are consistent with expected behavior.
Debug	Information that is useful when performing detailed troubleshooting procedures.

By default, log entries that are assigned a critical or warning level remain in the log after a switch reboot. Issuing a clear log command does not remove these static entries. To remove log entries of all levels (including warning or critical), use the following command:

```
clear log static
```

- **Subsystem** — The subsystem refers to the specific functional area to which the error refers. Table 50 describes the subsystems.

**Table 50:** Fault Log Subsystems

Subsystem	Description
Syst	General system-related information. Examples include memory, power supply, security violations, fan failure, overheat condition, and configuration mode.
STP	STP information. Examples include an STP state change.
Brdg	Bridge-related functionality. Examples include low table space and queue overflow.
SNMP	SNMP information. Examples include community string violations.
Telnet	Information related to Telnet login and configuration performed by way of a Telnet session.
VLAN	VLAN-related configuration information.

**Table 50:** Fault Log Subsystems (continued)

Subsystem	Description
Port	Port management-related configuration. Examples include port statistics and errors.

- **Message** — The message contains the log information with text that is specific to the problem.

## Local Logging

The switch maintains 1,000 messages in its internal log. You can display a snapshot of the log at any time by using the following command:

```
show log {<priority>}
```

where the following is true:

- `priority` — Filters the log to display message with the selected priority or higher (more critical). Priorities include (in order) critical, emergency, alert, error, warning, notice, info, and debug. If not specified, all messages are displayed.

## Real-Time Display

In addition to viewing a snapshot of the log, you can configure the system to maintain a running real-time display of log messages on the console. To turn on the log display, use the following command:

```
enable log display
```

To configure the log display, use the following command:

```
config log display {<priority>}
```

If `priority` is not specified, only messages of critical priority are displayed.

If you enable the log display on a terminal connected to the console port, your settings will remain in effect even after your console session is ended (unless you explicitly disable the log display).

When using a Telnet connection, if your Telnet session is disconnected (because of the inactivity timer, or for other reasons), the log display is automatically halted. You must restart the log display by using the `enable log display` command.

## Remote Logging

In addition to maintaining an internal log, the switch supports remote logging by way of the UNIX syslog host facility. To enable remote logging, follow these steps:

- 1 Configure the syslog host to accept and log messages.
- 2 Enable remote logging by using the following command:

```
enable syslog
```

- 3 Configure remote logging by using the following command:

```
config syslog {add} <ipaddress> <facility> {<priority>}
```

Specify the following:

- `ipaddress` — The IP address of the syslog host.
- `facility` — The syslog facility level for local use. Options include `local0` through `local7`.
- `priority` — Filters the log to display message with the selected priority or higher (more critical). Priorities include (in order) `critical`, `emergency`, `alert`, `error`, `warning`, `notice`, `info`, and `debug`. If not specified, only critical priority messages are sent to the syslog host.

**NOTE**

Refer to your UNIX documentation for more information about the syslog host facility.

## Logging Configuration Changes

ExtremeWare allows you to record all configuration changes and their sources that are made using the CLI by way of Telnet or the local console. The changes are logged to the system log. Each log entry includes the user account name that performed the change and the source IP address of the client (if Telnet was used). Configuration logging applies only to commands that result in a configuration change. To enable configuration logging, use the following command:

```
enable cli-config-logging
```

To disable configuration logging, use the following command:

```
disable cli-config-logging
```

CLI configuration logging is enabled by default.

## Logging Commands

The commands described in Table 51 allow you to configure logging options, reset logging options, display the log, and clear the log.

**Table 51:** Logging Commands

Command	Description
<code>clear counters</code>	Clears all switch statistics and port counters.
<code>clear log {static}</code>	Clears the log. If <code>static</code> is specified, the critical log messages are also cleared.
<code>config log display {&lt;priority&gt;}</code>	Configures the real-time log display. Options include: <ul style="list-style-type: none"> <li>• <code>priority</code> — Filters the log to display messages with the selected priority or higher (more critical). Priorities include <code>critical</code>, <code>emergency</code>, <code>error</code>, <code>alert</code>, <code>warning</code>, <code>notice</code>, <code>info</code>, and <code>debug</code>. If not specified, informational priority messages and higher are displayed.</li> </ul>

**Table 51:** Logging Commands (continued)

Command	Description
config syslog {add} <host name/ip> {<port>} <facility> {<priority>}	Configures the syslog host address and filters messages sent to the syslog host. Up to 4 syslog servers can be configured. Options include: <ul style="list-style-type: none"> <li>• <code>host name/ip</code>— The IP address or name of the syslog host.</li> <li>• <code>port</code> — The port of the syslog host.</li> <li>• <code>facility</code> — The syslog facility level for local use (local0 - local7).</li> <li>• <code>priority</code> — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, only critical priority messages and are sent to the syslog host.</li> </ul>
config syslog delete <host name/ip> {<port>} <facility> {<priority>}	Deletes a syslog host address. <ul style="list-style-type: none"> <li>• <code>facility</code> — The syslog facility level for local use (local0 - local7).</li> <li>• <code>priority</code> — Filters the log to display messages with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, only critical priority messages and are sent to the syslog host.</li> </ul>
disable cli-config-logging	Disables configuration logging.
disable log display	Disables the log display.
disable syslog	Disables logging to a remote syslog host.
enable cli-config-logging	Enables the logging of CLI configuration commands to the Syslog for auditing purposes. The default setting is enabled.
enable log display	Enables the log display.
enable syslog	Enables logging to a remote syslog host.
show log {<priority>}	Displays the current snapshot of the log. Options include: <ul style="list-style-type: none"> <li>• <code>priority</code> — Filters the log to display message with the selected priority or higher (more critical). Priorities include critical, emergency, alert, error, warning, notice, info, and debug. If not specified, all messages are displayed.</li> </ul>
show log config	Displays the log configuration, including the syslog host IP address, the priority level of messages being logged locally, and the priority level of messages being sent to the syslog host.

# RMON

Using the Remote Monitoring (RMON) capabilities of the switch allows network administrators to improve system efficiency and reduce the load on the network.

The following sections explain more about the RMON concept and the RMON features supported by the switch.



---

*You can only use the RMON features of the system if you have an RMON management application, and have enabled RMON on the switch.*

## About RMON

RMON is the common abbreviation for the Remote Monitoring Management Information Base (MIB) system defined by the Internet Engineering Task Force (IETF) documents RFC 1271 and RFC 1757, which allows you to monitor LANs remotely.

A typical RMON setup consists of the following two components:

- **RMON probe** — An intelligent, remotely controlled device or software agent that continually collects statistics about a LAN segment or VLAN. The probe transfers the information to a management workstation on request, or when a predefined threshold is crossed.
- **Management workstation** — Communicates with the RMON probe and collects the statistics from it. The workstation does not have to be on the same network as the probe, and can manage the probe by in-band or out-of-band connections.

## RMON Features of the Switch

The IETF defines nine groups of Ethernet RMON statistics. The switch supports the following four of these groups:

- Statistics
- History
- Alarms
- Events

This section describes these groups and discusses how they can be used.

### Statistics

The RMON Ethernet Statistics group provides traffic and error statistics showing packets, bytes, broadcasts, multicasts, and errors on a LAN segment or VLAN.

Information from the Statistics group is used to detect changes in traffic and error patterns in critical areas of the network.

## History

The History group provides historical views of network performance by taking periodic samples of the counters supplied by the Statistics group. The group features user-defined sample intervals and bucket counters for complete customization of trend analysis.

The group is useful for analysis of traffic patterns and trends on a LAN segment or VLAN, and to establish baseline information indicating normal operating parameters.

## Alarms

The Alarms group provides a versatile, general mechanism for setting threshold and sampling intervals to generate events on any RMON variable. Both rising and falling thresholds are supported, and thresholds can be on the absolute value of a variable or its delta value. In addition, alarm thresholds can be autocalibrated or set manually.

Alarms inform you of a network performance problem and can trigger automated action responses through the Events group.

## Events

The Events group creates entries in an event log and/or sends SNMP traps to the management workstation. An event is triggered by an RMON alarm. The action taken can be configured to ignore it, to log the event, to send an SNMP trap to the receivers listed in the trap receiver table, or to both log and send a trap. The RMON traps are defined in RFC 1757 for rising and falling thresholds.

Effective use of the Events group saves you time. Rather than having to watch real-time graphs for important occurrences, you can depend on the Event group for notification. Through the SNMP traps, events can trigger other actions, which provides a mechanism for an automated response to certain occurrences.

## Configuring RMON

RMON requires one probe per LAN segment, and standalone RMON probes traditionally have been expensive. Therefore, Extreme's approach has been to build an inexpensive RMON probe into the agent of each system. This allows RMON to be widely deployed around the network without costing more than traditional network management. The switch accurately maintains RMON statistics at the maximum line rate of all of its ports.

For example, statistics can be related to individual ports. Also, because a probe must be able to see all traffic, a stand-alone probe must be attached to a nonsecure port. Implementing RMON in the switch means that all ports can have security features enabled.

To enable or disable the collection of RMON statistics on the switch, use the following command:

```
[enable | disable] rmon
```

By default, RMON is disabled. However, even in the disabled state, the switch response to RMON queries and sets for alarms and events. By enabling RMON, the switch begins the processes necessary for collecting switch statistics.

## Event Actions

The actions that you can define for each alarm are shown in Table 52.

**Table 52:** Event Actions

Action	High Threshold
No action	
Notify only	Send trap to all trap receivers.
Notify and log	Send trap; place entry in RMON log.

To be notified of events using SNMP traps, you must configure one or more trap receivers, as described in Chapter 3, “Managing the Switch”.



# 13

## Spanning Tree Protocol (STP)

---

This chapter describes the following topics:

- Overview of the Spanning Tree Protocol on page 145
- Spanning Tree Domains on page 145
- STP Configurations on page 146
- Configuring STP on the Switch on page 148
- Displaying STP Settings on page 151
- Disabling and Resetting STP on page 152

Using the Spanning Tree Protocol (STP) functionality of the switch makes your network more fault tolerant. The following sections explain more about STP and the STP features supported by ExtremeWare.



---

*STP is a part of the 802.1D bridge specification defined by the IEEE Computer Society. To explain STP in terms used by the 802.1D specification, the switch will be referred to as a bridge.*

### Overview of the Spanning Tree Protocol

STP is a bridge-based mechanism for providing fault tolerance on networks. STP allows you to implement parallel paths for network traffic, and ensure that:

- Redundant paths are disabled when the main paths are operational.
- Redundant paths are enabled if the main path fails.

### Spanning Tree Domains

The switch can be partitioned into multiple virtual bridges. Each virtual bridge can run an independent Spanning Tree instance. Each Spanning Tree instance is called a *Spanning Tree Domain* (STPD). Each STPD has its own root bridge and active path. Once the STPD is created, one or more VLANs can be assigned to it.

A port can belong to only one STPD. If a port is a member of multiple VLANs, then all those VLANs must belong to the same STPD.

The key points to remember when configuring VLANs and STP are:

- Each VLAN forms an independent broadcast domain
- STP blocks paths to create a loop-free environment
- When STP blocks a path, no data can be transmitted or received on the blocked port
- Within any given STPD, all VLANs belonging to it use the same spanning tree



## NOTE

Ensure that multiple STPD instances within a single switch do not see each other in the same broadcast domain. This could happen if, for example, another external bridge is used to connect VLANs belonging to separate STPDs.

If you delete an STPD, the VLANs that were members of that STPD are also deleted. You must remove all VLANs associated with the STP before deleting the STPD.

## Defaults

The default device configuration contains a single STPD called *s0*. The default VLAN is a member of STPD *s0*.

All STP parameters default to the IEEE 802.1D values, as appropriate.

## STPD BPDU Tunneling

You can configure ExtremeWare to allow a BPDU to traverse a VLAN without being processed by STP, even if STP is enabled on the port. This is known as BPDU *tunneling*.

To enable and disable BPDU tunneling on a VLAN, use the following command:

```
[enable | disable] ignore-bpdu vlan <name>
```

If you have a known topology and have switches outside of your network within your STPD, use this feature to keep the root bridge within your network.

## STP Configurations

When you assign VLANs to an STPD, pay careful attention to the STP configuration and its effect on the forwarding of VLAN traffic.

Figure 15 illustrates a network that uses VLAN tagging for trunk connections. The following four VLANs have been defined:

- *Sales* is defined on switch A, switch B, and switch M.
- *Personnel* is defined on switch A, switch B, and switch M.
- *Manufacturing* is defined on switch Y, switch Z, and switch M.
- *Engineering* is defined on switch Y, switch Z, and switch M.

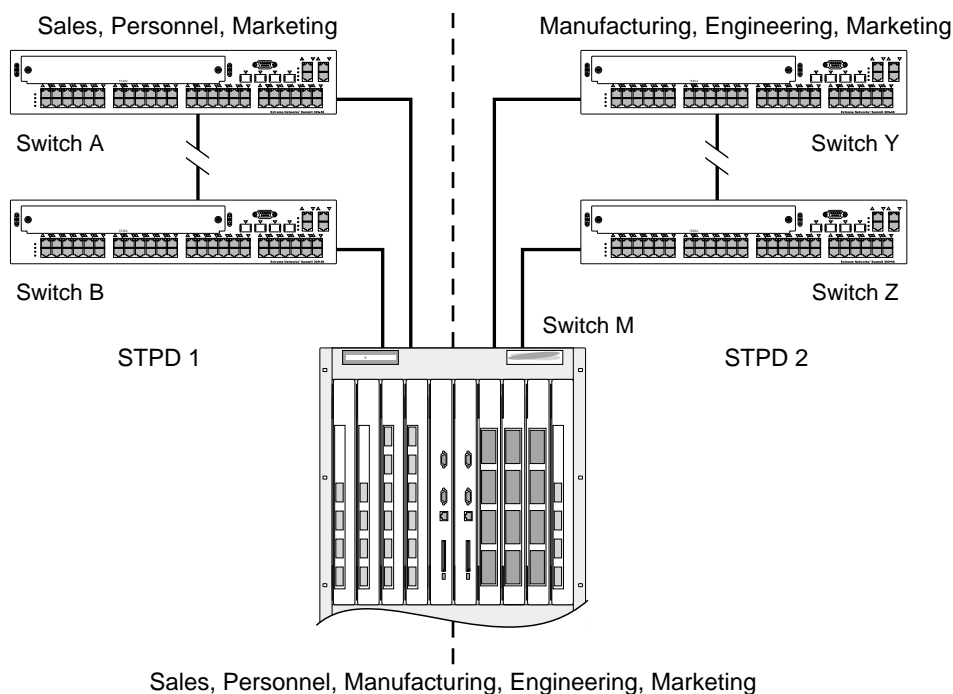
- *Marketing* is defined on all switches (switch A, switch B, switch Y, switch Z, and switch M).

Two STPDs are defined:

- STPD1 contains VLANs *Sales* and *Personnel*.
- STPD2 contains VLANs *Manufacturing* and *Engineering*.

The VLAN *Marketing* is a member of the default STPD, but not assigned to either STPD1 or STPD2.

**Figure 15:** Multiple Spanning Tree Domains

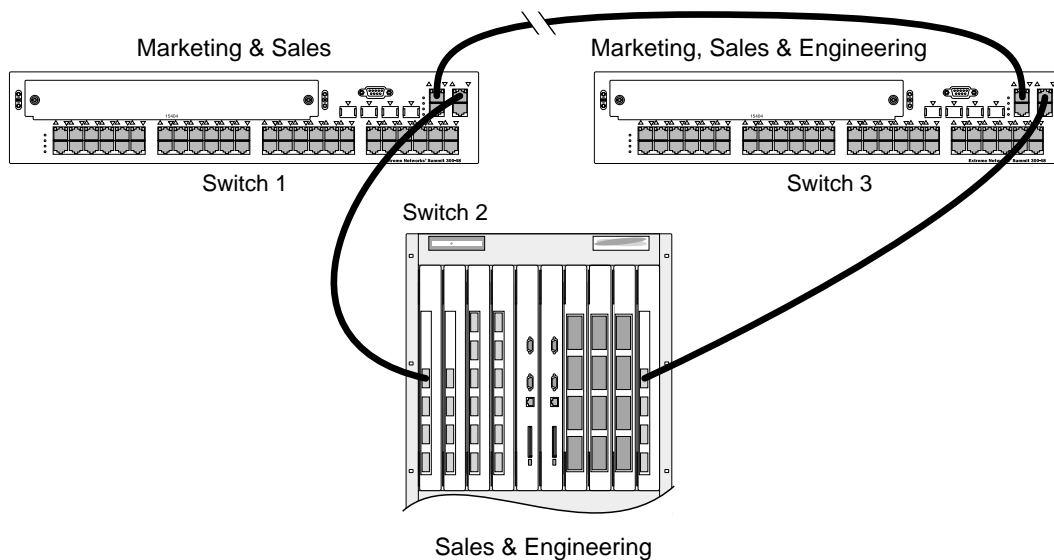


When the switches in this configuration start up, STP configures each STPD such that there are no active loops in the topology. STP could configure the topology in a number of ways to make it loop-free.

In Figure 15, the connection between switch A and switch B is put into blocking state, and the connection between switch Y and switch Z is put into blocking state. After STP converges, all the VLANs can communicate, and all bridging loops are prevented.

The VLAN *Marketing*, which has not been assigned to either STPD1 or STPD2, communicates using all five switches. The topology has no loops, because STP has already blocked the port connection between switch A and switch B, and between switch Y and switch Z.

Within a single STPD, you must be extra careful when configuring your VLANs. Figure 16 illustrates a network that has been incorrectly set up using a single STPD so that the STP configuration disables the ability of the switches to forward VLAN traffic.

**Figure 16:** Tag-based STP configuration

LB48015

The tag-based network in Figure 16 has the following configuration:

- Switch 1 contains VLAN *Marketing* and VLAN *Sales*.
- Switch 2 contains VLAN *Engineering* and VLAN *Sales*.
- Switch 3 contains VLAN *Marketing*, VLAN *Engineering*, and VLAN *Sales*.
- The tagged trunk connections for three switches form a triangular loop that is not permitted in an STP topology.
- All VLANs in each switch are members of the same STPD.

STP can block traffic between switch 1 and switch 3 by disabling the trunk ports for that connection on each switch.

Switch 2 has no ports assigned to VLAN *marketing*. Therefore, if the trunk for VLAN *marketing* on switches 1 and 3 is blocked, the traffic for VLAN *marketing* will not be able to traverse the switches.

## Configuring STP on the Switch

To configure STP, follow these steps:

- 1 Create one or more STP domains using the following command:

```
create stpd <stpd_name>
```



### NOTE

STPD, VLAN, and QoS profile names must all be unique. For example, a name used to identify a VLAN cannot be used when you create an STPD or a QoS profile.

- 2 Add one or more VLANs to the STPD using the following command:

```
config stpd <stpd_name> add vlan <name>
```

### 3 Enable STP for one or more STP domains using the following command:

```
enable stpd {<stpd_name>}
```



#### NOTE

All VLANs belong to the default STPD (s0). If you do not want to run STP on a VLAN, you must add the VLAN to a STPD that is disabled.

Once you have created the STPD, you can optionally configure STP parameters for the STPD.



#### CAUTION

You should not configure any STP parameters unless you have considerable knowledge and experience with STP. The default STP parameters are adequate for most networks.

The following parameters can be configured on each STPD:

- Hello time
- Forward delay
- Max age
- Bridge priority

The following parameters can be configured on each port:

- Path cost
- Port priority



#### NOTE

The device supports the RFC 1493 Bridge MIB. Parameters of only the s0 default STPD are accessible through this MIB.

Table 53 shows the commands used to configure STP.

**Table 53:** STP Configuration Commands

Command	Description
config stpd <stpd_name> add vlan <name>	Adds a VLAN to the STPD.
config stpd <stpd_name> forwarddelay <value>	Specifies the time (in seconds) that the ports in this STPD spend in the listening and learning states when the switch is the Root Bridge.  The range is 4 through 30. The default setting is 15 seconds.
config stpd <stpd_name> hellotime <value>	Specifies the time delay (in seconds) between the transmission of BPDUs from this STPD when it is the Root Bridge.  The range is 1 through 10. The default setting is 2 seconds.

**Table 53:** STP Configuration Commands (continued)

Command	Description
config stpd <stpd_name> maxage <value>	<p>Specifies the maximum age of a BPDU in this STPD.</p> <p>The range is 6 through 40. The default setting is 20 seconds.</p> <p>Note that the time must be greater than, or equal to <math>2 * (\text{Hello Time} + 1)</math> and less than, or equal to <math>2 * (\text{Forward Delay} - 1)</math>.</p>
config stpd <stpd_name> ports cost <value> <portlist>	<p>Specifies the path cost of the port in this STPD.</p> <p>The range is 1 through 65,535. The switch automatically assigns a default path cost based on the speed of the port, as follows:</p> <ul style="list-style-type: none"> <li>• For a 10 Mbps port, the default cost is 100.</li> <li>• For a 100 Mbps port, the default cost is 19.</li> </ul>
config stpd <stpd_name> ports priority <value> <portlist>	<p>Specifies the priority of the port in this STPD. By changing the priority of the port, you can make it more or less likely to become the root port.</p> <p>The range is 0 through 31. The default setting is 16. A setting of 0 indicates the lowest priority.</p>
config stpd <stpd_name> priority <value>	<p>Specifies the priority of the STPD. By changing the priority of the STPD, you can make it more or less likely to become the root bridge.</p> <p>The range is 0 through 65,535. The default setting is 32,768. A setting of 0 indicates the highest priority.</p>
create stpd <stpd_name>	<p>Creates an STPD. When created, an STPD has the following default parameters:</p> <ul style="list-style-type: none"> <li>• Bridge priority — 32,768</li> <li>• Hello time — 2 seconds</li> <li>• Forward delay — 15 seconds</li> </ul>
enable ignore-bpdu vlan <name>	<p>Configures the switch to ignore STP BPDUs, which prevents ports in the VLAN from becoming part of an STPD. This command is useful when you have a known topology with switches outside your network, and wish to keep the root bridge within your network. The default setting is disabled.</p>
enable ignore-stp vlan <vlan name>	<p>Configures the switch to ignore the STP protocol, and not block traffic for the VLAN(s). This command is useful when multiple VLANs share the same physical ports, but only some of the VLANs require STP protection. The default setting is disabled.</p>
enable stpd {<stpd_name>}	<p>Enables the STP protocol for one or all STPDs. The default setting is disabled.</p>
enable stpd ports {<portlist>}	<p>Enables the STP protocol on one or more ports. If STPD is enabled for a port, bridge protocol data units (BPDUs) will be generated on that port if STP is enabled for the associated STPD. The default setting is enabled.</p>

## STP Configuration Example

The following Summit 300-48 switch example creates and enables an STPD named *Backbone\_st*. It assigns the *Manufacturing* VLAN to the STPD. It disables STP on ports 1:1 through 1:7 and port 1:12.

```
create stpd backbone_st
config stpd backbone_st add vlan manufacturing
enable stpd backbone_st
disable stpd backbone_st port 1:1-1:7,1:12
```

## Displaying STP Settings

To display STP settings, use the following command:

```
show stpd {<stpd_name>}
```

This command displays the following information:

- STPD name
- Bridge ID
- STPD configuration information

To display the STP state of a port, use the following command:

```
show stpd <stpd_name> port <portlist>
```

This command displays the following information:

- STPD port configuration
- STPD state (root bridge, and so on)
- STPD port state (forwarding, blocking, and so on)

## Disabling and Resetting STP

To disable STP or return STP settings to their defaults, use the commands listed in Table 54.

**Table 54:** STP Disable and Reset Commands

Command	Description
delete stpd <stpd_name>	Removes an STPD. An STPD can only be removed if all VLANs have been deleted from it. The default STPD, s0, cannot be deleted.
disable ignore-bpdu vlan <name>	Allows the switch to recognize STP BPDUs.
disable ignore-stp vlan <name>	Allows a VLAN to use STP port information.
disable stpd [<stpd_name>   all]	Disables the STP mechanism on a particular STPD, or for all STPDs.
disable stpd ports <portlist>	Disables STP on one or more ports. Disabling STP on one or more ports puts those ports in <i>forwarding</i> state; all BPDUs received on those ports will be disregarded.
unconfig stpd {<stpd_name>}	Restores default STP values to a particular STPD or to all STPDs.



# 14

# IP Unicast Routing

---

This chapter describes the following topics:

- Overview of IP Unicast Routing on page 153
- Proxy ARP on page 156
- Relative Route Priorities on page 157
- Configuring IP Unicast Routing on page 157
- IP Commands on page 158
- Routing Configuration Example on page 162
- Displaying Router Settings on page 163
- Resetting and Disabling Router Settings on page 163
- Configuring DHCP/BOOTP Relay on page 164
- UDP-Forwarding on page 165

This chapter assumes that you are already familiar with IP unicast routing. If not, refer to the following publications for additional information:

- RFC 1256 — *ICMP Router Discovery Messages*
- RFC 1812 — *Requirements for IP Version 4 Routers*

## Overview of IP Unicast Routing

The switch provides full layer 3, IP unicast routing. The switch dynamically builds and maintains a routing table, and determines the best path for each of its static route entries.

Each host using the IP unicast routing functionality of the switch must have a unique IP address assigned. In addition, the default gateway assigned to the host must be the IP address of the router interface.

## Router Interfaces

The routing software and hardware routes IP traffic between router interfaces. A router interface is simply a VLAN that has an IP address assigned to it.

As you create VLANs with IP addresses belonging to different IP subnets, you can also choose to route between the VLANs. Both the VLAN switching and IP routing function occur within the switch.

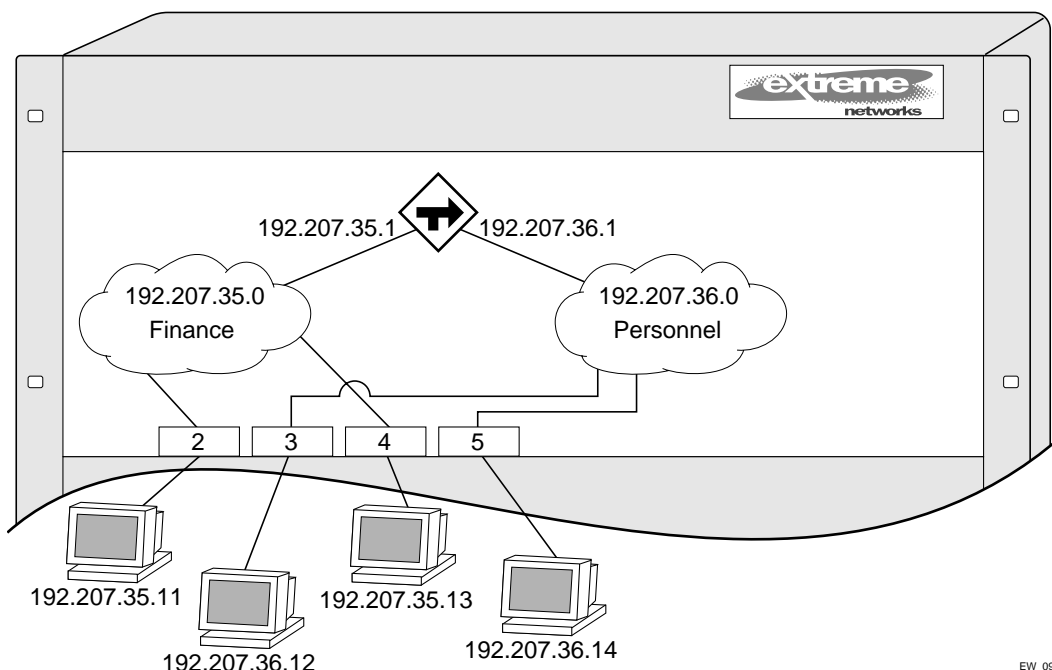


### NOTE

Each IP address and mask assigned to a VLAN must represent a unique IP subnet. You cannot configure the same IP address and subnet on different VLANs.

In Figure 17, a Summit 300-48 switch is depicted with two VLANs defined; *Finance* and *Personnel*. Ports 2 and 4 are assigned to *Finance*; ports 3 and 5 are assigned to *Personnel*. *Finance* belongs to the IP network 192.207.35.0; the router interface for *Finance* is assigned the IP address 192.207.35.1. *Personnel* belongs to the IP network 192.207.36.0; its router interface is assigned IP address 192.207.36.1. Traffic within each VLAN is switched using the Ethernet MAC addresses. Traffic between the two VLANs is routed using the IP addresses.

**Figure 17:** Routing between VLANs



EW\_090

## Populating the Routing Table

The switch maintains an IP routing table for both network routes and host routes. The table is populated from the following sources:

- Dynamically, by way of routing protocol packets or by ICMP redirects exchanged with other routers
- Statically, by way of routes entered by the administrator
  - Default routes, configured by the administrator

- Locally, by way of interface addresses assigned to the system
- By other static routes, as configured by the administrator

## NOTE

If you define a default route, and subsequently delete the VLAN on the subnet associated with the default route, the invalid default route entry remains. You must manually delete the configured default route.

## Static Routes

Static routes are manually entered into the routing table. Static routes are used to reach networks not advertised by routers.

Static routes can also be used for security reasons, to control which routes you want advertised by the router. The default setting is disabled. Static routes are never aged out of the routing table.

A static route must be associated with a valid IP subnet. An IP subnet is associated with a single VLAN by its IP address and subnet mask. If the VLAN is subsequently deleted, the static route entries using that subnet must be deleted manually.

## Multiple Routes

When there are multiple, conflicting choices of a route to a particular destination, the router picks the route with the longest matching network mask. If these are still equal, the router picks the route using the following criteria (in the order specified):

- Directly attached network interfaces
- ICMP redirects (refer to Table 58, later in this chapter)
- Static routes
- Directly attached network interfaces that are not active.



If you define multiple default routes, the route that has the lowest metric is used. If multiple default routes have the same lowest metric, the system picks one of the routes.

You can also configure *blackhole* routes — traffic to these destinations is silently dropped.

## IP Route Sharing

IP route sharing allows multiple equal-cost routes to be used concurrently. IP route sharing can be used with static routes. To use IP route sharing, use the following command:

```
enable iproute sharing
```

Next, configure static routes as you would normally. ExtremeWare supports unlimited route sharing across static routes.

Route sharing is useful only in instances where you are constrained for bandwidth. This is typically not the case using Extreme switches. Using route sharing makes router troubleshooting more difficult because of the complexity in predicting the path over which the traffic will travel.

## Proxy ARP

Proxy Address Resolution Protocol (ARP) was first invented so that ARP-capable devices could respond to ARP Request packets on behalf of ARP-incapable devices. Proxy ARP can also be used to achieve router redundancy and simplify IP client configuration. The switch supports proxy ARP for this type of network configuration. The section describes some example of how to use proxy ARP with the switch.

### ARP-Incapable Devices

To configure the switch to respond to ARP Requests on behalf of devices that are incapable of doing so, you must configure the IP address and MAC address of the ARP-incapable device using the use the following command:

```
config iparp add proxy <ipaddress> {<mask>} <mac_address> {always}
```

Once configured, the system responds to ARP Requests on behalf of the device as long as the following conditions are satisfied:

- The valid IP ARP Request is received on a router interface.
- The target IP address matches the IP address configured in the proxy ARP table.
- The proxy ARP table entry indicates that the system should always answer this ARP Request, regardless of the ingress VLAN (the `always` parameter must be applied).

Once all the proxy ARP conditions are met, the switch formulates an ARP Response using the configured MAC address in the packet.

### Proxy ARP Between Subnets

In some networks, it is desirable to configure the IP host with a wider subnet than the actual subnet mask of the segment. Proxy ARP can be used so that the router answers ARP Requests for devices outside of the subnet. As a result, the host communicates as if all devices are local. In reality, communication with devices outside of the subnet are proxied by the router.

For example, an IP host is configured with a class B address of 100.101.102.103 and a mask of 255.255.0.0. The switch is configured with the IP address 100.101.102.1 and a mask of 255.255.255.0. The switch is also configured with a proxy ARP entry of IP address 100.101.0.0 and mask 255.255.0.0, *without* the `always` parameter.

When the IP host tries to communicate with the host at address 100.101.45.67, the IP hosts communicates as if the two hosts are on the same subnet, and sends out an IP ARP Request. The switch answers on behalf of the device at address 100.101.45.67, using its own MAC address. All subsequent data packets from 100.101.102.103 are sent to the switch, and the switch routes the packets to 100.101.45.67.

## Relative Route Priorities

Table 55 lists the relative priorities assigned to routes depending upon the learned source of the route.



### CAUTION

*Although these priorities can be changed, do not attempt any manipulation unless you are expertly familiar with the possible consequences.*

**Table 55:** Relative Route Priorities

Route Origin	Priority
Direct	10
BlackHole	50
Static	1100
ICMP	1200
BOOTP	5000

To change the relative route priority, use the following command:

```
config iproute priority [ bootp | icmp | static ] <priority>
```

## Configuring IP Unicast Routing

This section describes the commands associated with configuring IP unicast routing on the switch. To configure routing, follow these steps:

- 1 Create and configure two or more VLANs.
- 2 Assign each VLAN that will be using routing an IP address using the following command:

```
config vlan <name> ipaddress <ipaddress> {<mask>}
```

Ensure that each VLAN has a unique IP address.

- 3 Configure a default route using the following command:

```
config iproute add default <gateway> {<metric>}
```

Default routes are used when the router has no other dynamic or static route to the requested destination.

- 4 Turn on IP routing for one or all VLANs using the following command:

```
enable ipforwarding {vlan <name>}
```

## Verifying the IP Unicast Routing Configuration

Use the `show iproute` command to display the current configuration of IP unicast routing for the switch, and for each VLAN. The `show iproute` command displays the currently configured routes, and includes how each route was learned.

Additional verification commands include:

- `show iparp` — Displays the IP ARP table of the system.
- `show ipfdb` — Displays the hosts that have been transmitting or receiving packets, and the port and VLAN for each host.
- `show ipconfig` — Displays configuration information for one or more VLANs.

## IP Commands

Table 56 describes the commands used to configure basic IP settings.

**Table 56:** Basic IP Commands

Command	Description
<code>clear iparp {&lt;ipaddress&gt; &lt;mask&gt;   vlan &lt;vlan&gt;}</code>	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
<code>clear ipfdb {&lt;ipaddress&gt; &lt;netmask&gt;   vlan &lt;name&gt;}</code>	Removes the dynamic entries in the IP forwarding database. If no options are specified, all dynamic IP FDB entries are removed.
<code>config bootprelay add &lt;ipaddress&gt;</code>	Adds the IP destination address to forward BOOTP packets.
<code>config bootprelay delete [&lt;ipaddress&gt;   all]</code>	Removes one or all IP destination addresses for forwarding BOOTP packets.
<code>config iparp add &lt;ipaddress&gt; &lt;mac_address&gt;</code>	Adds a permanent entry to the ARP table. Specify the IP address and MAC address of the entry.
<code>config iparp add proxy &lt;ipaddress&gt; {&lt;mask&gt;} {&lt;mac_address&gt;} {always}</code>	Configures proxy ARP entries. When <code>mask</code> is not specified, an address with the mask 255.255.255.255 is assumed. When <code>mac_address</code> is not specified, the MAC address of the switch is used in the ARP Response. When <code>always</code> is specified, the switch answers ARP Requests without filtering requests that belong to the same subnet of the receiving router interface.
<code>config iparp delete &lt;ipaddress&gt;</code>	Deletes an entry from the ARP table. Specify the IP address of the entry.
<code>config iparp delete proxy [&lt;ipaddress&gt; {&lt;mask&gt;}   all]</code>	Deletes one or all proxy ARP entries.
<code>config iparp timeout &lt;minutes&gt;</code>	Configures the IP ARP timeout period. The default setting is 20 minutes. A setting of 0 disables ARP aging. The maximum aging time is 32,767 minutes.

**Table 56:** Basic IP Commands (continued)

Command	Description
disable bootp vlan [<name>   all]	Disables the generation and processing of BOOTP packets.
disable bootprelay	Disables the forwarding of BOOTP requests.
disable ipforwarding {vlan <name>}	Disables routing for one or all VLANs.
disable ipforwarding broadcast {vlan <name>}	Disables routing of broadcasts to other networks.
disable loopback-mode vlan [<name>   all]	Disables loopback-mode on an interface.
enable bootp vlan [<name>   all]	Enables the generation and processing of BOOTP packets on a VLAN to obtain an IP address for the VLAN from a BOOTP server. The default setting is enabled for all VLANs.
enable bootprelay	Enables the forwarding of BOOTP and Dynamic Host Configuration Protocol (DHCP) requests.
enable ipforwarding {vlan <name>}	Enables IP routing for one or all VLANs. If no argument is provided, enables routing for all VLANs that have been configured with an IP address. The default setting for <code>ipforwarding</code> is disabled.
enable ipforwarding broadcast {vlan <name>}	Enables forwarding IP broadcast traffic for one or all VLANs. If no argument is provided, enables broadcast forwarding for all VLANs. To enable, <code>ipforwarding</code> must be enabled on the VLAN. The default setting is disabled.
enable loopback-mode vlan [<name>   all]	Enables a loopback mode on an interface. If loopback is enabled, the router interface remains in the UP state, even if no ports are defined in the VLAN. As a result, the subnet is always advertised as one of the available routes.

Table 57 describes the commands used to configure the IP route table.

**Table 57:** Route Table Configuration Commands

Command	Description
config iproute add <ipaddress> <mask> <gateway> <metric>	Adds a static address to the routing table. Use a value of 255.255.255.255 for <code>mask</code> to indicate a host entry.
config iproute add blackhole <ipaddress> <mask>	Adds a <code>blackhole</code> address to the routing table. All traffic destined for the configured IP address is dropped, and no Internet Control Message Protocol (ICMP) message is generated.

**Table 57:** Route Table Configuration Commands (continued)

Command	Description
config iproute add default <gateway> {<metric>}	Adds a default gateway to the routing table. A default gateway must be located on a configured IP interface. If no metric is specified, the default metric of 1 is used. Use the unicast-only or multicast-only options to specify a particular traffic type. If not specified, both unicast and multicast traffic uses the default route.
config iproute delete <ipaddress> <mask> <gateway>	Deletes a static address from the routing table.
config iproute delete blackhole <ipaddress> <mask>	Deletes a blackhole address from the routing table.
config iproute delete default <gateway>	Deletes a default gateway from the routing table.
config iproute priority [ bootp   icmp   static ] <priority>	Changes the priority for all routes from a particular route origin.
disable iproute sharing	Disables load sharing for multiple routes.
enable iproute sharing	Enables load sharing if multiple routes to the same destination are available. Only paths with the same lowest cost are shared. The default setting is disabled.
rtlookup [<ipaddress>   <hostname>]	Performs a look-up in the route table to determine the best route to reach an IP address.

Table 58 describes the commands used to configure IP options and the ICMP protocol.

**Table 58:** ICMP Configuration Commands

Command	Description
config irdp [multicast   broadcast]	Configures the destination address of the router advertisement messages. The default setting is <code>multicast</code> .
config irdp <mininterval> <maxinterval> <lifetime> <preference>	Configures the router advertisement message timers, using seconds. Specify: <ul style="list-style-type: none"> <li><code>mininterval</code> — The minimum amount of time between router advertisements. The default setting is 450 seconds.</li> <li><code>maxinterval</code> — The maximum time between router advertisements. The default setting is 600 seconds.</li> <li><code>lifetime</code> — The default setting is 1,800 seconds.</li> <li><code>preference</code> — The preference level of the router. An ICMP Router Discover Protocol (IRDP) client always uses the router with the highest preference level. Change this setting to encourage or discourage the use of this router. The default setting is 0.</li> </ul>
disable icmp parameter-problem {vlan <name>}	Disables the generation of ICMP messages for the parameter problem packet type.



**Table 58: ICMP Configuration Commands (continued)**

Command	Description
disable ip-option loose-source-route	Disables the loose source route IP option.
disable ip-option record-route	Disables the record route IP option.
disable ip-option record-timestamp	Disables the record timestamp IP option.
disable ip-option strict-source-route	Disables the strict source route IP option.
disable ip-option use-router-alert	Disables the generation of the router alert IP option.
enable icmp address-mask {vlan <name>}	Enables the generation of an ICMP address-mask reply (type 18, code 0) when an ICMP address mask request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp parameter-problem {vlan <name>}	Enables the generation of an ICMP parameter-problem message (type 12) when the switch cannot properly process the IP header or IP option information. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp redirects {vlan <name>}	Enables the generation of an ICMP redirect message (type 5) when a packet must be forwarded out on the ingress port. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp time-exceeded {vlan <name>}	Enables the generation of an ICMP time exceeded message (type 11) when the TTL field expires during forwarding. IP multicast packets do not trigger ICMP time exceeded messages. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp timestamp {vlan <name>}	Enables the generation of an ICMP timestamp response (type 14, code 0) when an ICMP timestamp request is received. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp unreachable {vlan <name>}	Enables the generation of ICMP network unreachable messages (type 3, code 0), and host unreachable messages (type 3, code 1) when a packet cannot be forwarded to the destination because of unreachable route or host. ICMP packet processing on one or all VLANs. The default setting is enabled. If a VLAN is not specified, the command applies to all IP interfaces.
enable icmp userredirects	Enables the modification of route table information when an ICMP redirect message is received. This option applies to the switch when it <i>is not configured for routing</i> . The default setting is disabled.
enable ip-option loose-source-route	Enables the loose source route IP option.
enable ip-option record-route	Enables the record route IP option.
enable ip-option record-timestamp	Enables the record timestamp IP option.
enable ip-option strict-source-route	Enables the strict source route IP option.

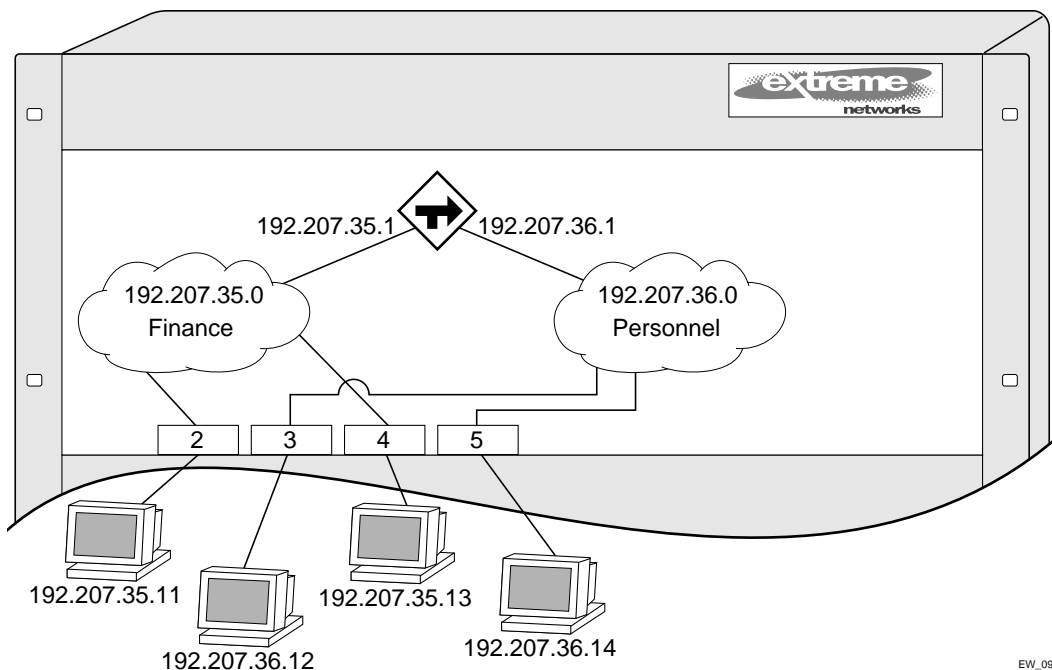
**Table 58:** ICMP Configuration Commands (continued)

Command	Description
enable ip-option use-router-alert	Enables the switch to generate the router alert IP option with routing protocol packets.
enable irdp {vlan <name>}	Enables the generation of ICMP router advertisement messages on one or all VLANs. The default setting is enabled.
unconfig icmp	Resets all ICMP settings to the default values.
unconfig irdp	Resets all router advertisement settings to the default values.

## Routing Configuration Example

Figure 18 illustrates a Summit24e3 switch that has two VLANs defined as follows:

- *Finance*
  - Contains ports 2 and 4.
  - IP address 192.207.35.1.
- *Personnel*
  - Contains ports 3 and 5.
  - IP address 192.207.36.1.

**Figure 18:** Unicast routing configuration example

In this configuration, all IP traffic from stations connected to ports 2 and 4 have access to the router by way of the VLAN *Finance*. Ports 3 and 5 reach the router by way of the VLAN *Personnel*.

The example in Figure 18 is configured as follows:

```
create vlan Finance
create vlan Personnel

config Finance add port 2,4
config Personnel add port 3,5

config Finance ipaddress 192.207.35.1
config Personnel ipaddress 192.207.36.1

enable ipforwarding
```

## Displaying Router Settings

To display settings for various IP routing components, use the commands listed in Table 59.

**Table 59:** Router Show Commands

Command	Description
show iparp {<ipaddress   vlan <name>   permanent}	Displays the IP Address Resolution Protocol (ARP) table. You can filter the display by IP address, VLAN, or permanent entries.
show iparp proxy {<ipaddress> {<mask>}}	Displays the proxy ARP table.
show ipconfig {vlan <name>}	Displays configuration information for one or all VLANs.
show ipconfig {vlan <name>} {detail}	Displays IP configuration settings.
show ipfdb {<ipaddress> <netmask>   vlan <name> }	Displays the contents of the IP forwarding database (FDB) table. If no option is specified, all IP FDB entries are displayed.
show ipstats {vlan <name>}	Displays IP statistics for the CPU of the system.

## Resetting and Disabling Router Settings

To return router settings to their defaults and disable routing functions, use the commands listed in Table 60

**Table 60:** Router Reset and Disable Commands

Command	Description
clear iparp {<ipaddress>   vlan <name>}	Removes dynamic entries in the IP ARP table. Permanent IP ARP entries are not affected.
clear ipfdb {<ipaddress> <netmask>   vlan <name>]	Removes the dynamic entries in the IP forwarding database. If no options are specified, all IP FDB entries are removed.
disable bootp vlan [<name>   all]	Disables the generation and processing of BOOTP packets.
disable bootprelay	Disables the forwarding of BOOTP requests.

**Table 60:** Router Reset and Disable Commands (continued)

Command	Description
<code>disable icmp address-mask {vlan &lt;name&gt;}</code>	Disables the generation of an ICMP address-mask reply messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp parameter-problem {vlan &lt;name&gt;}</code>	Disables the generation of ICMP parameter-problem messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp port-unreachables {vlan &lt;name&gt;}</code>	Disables the generation of ICMP port unreachable messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp redirects {vlan &lt;name&gt;}</code>	Disables the generation of ICMP redirect messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp time-exceeded {vlan &lt;name&gt;}</code>	Disables the generation of ICMP time exceeded messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp timestamp {vlan &lt;name&gt;}</code>	Disables the generation of ICMP timestamp response messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp unreachable {vlan &lt;name&gt;}</code>	Disables the generation of ICMP network unreachable messages and host unreachable messages. If a VLAN is not specified, the command applies to all IP interfaces.
<code>disable icmp userredirects</code>	Disables the changing of routing table information when an ICMP redirect message is received.
<code>disable ipforwarding {vlan &lt;name&gt;}</code>	Disables routing for one or all VLANs.
<code>disable ipforwarding broadcast {vlan &lt;name&gt;}</code>	Disables routing of broadcasts to other networks.
<code>disable irdp {vlan &lt;name&gt;}</code>	Disables the generation of router advertisement messages on one or all VLANs.
<code>unconfig icmp</code>	Resets all ICMP settings to the default values.
<code>unconfig irdp</code>	Resets all router advertisement settings to the default values.

## Configuring DHCP/BOOTP Relay

Once IP unicast routing is configured, you can configure the switch to forward Dynamic Host Configuration Protocol (DHCP) or BOOTP requests coming from clients on subnets being serviced by the switch and going to hosts on different subnets. This feature can be used in various applications, including DHCP services between Windows NT servers and clients running Windows 95. To configure the relay function, follow these steps:

- 1 Configure VLANs and IP unicast routing.
- 2 Enable the DHCP or BOOTP relay function, using the following command:

```
enable bootprelay
```

- 3 Configure the addresses to which DHCP or BOOTP requests should be directed, using the following command:

```
config bootprelay add <ipaddress>
```

To delete an entry, use the following command:

```
config bootprelay delete {<ipaddress> | all}
```

## Verifying the DHCP/BOOTP Relay Configuration

To verify the DHCP/BOOTP relay configuration, use the following command:

```
show ipconfig
```

This command displays the configuration of the BOOTP relay service, and the addresses that are currently configured.

## UDP-Forwarding

UDP-forwarding is a flexible and generalized routing utility for handling the directed forwarding of broadcast UDP packets. UDP-forwarding allows applications, such as multiple DHCP relay services from differing sets of VLANs, to be directed to different DHCP servers. The following rules apply to UDP broadcast packets handled by this feature:

- If the UDP profile includes BOOTP or DHCP, it is handled according to guidelines in RFC 1542.
- If the UDP profile includes other types of traffic, these packets have the IP destination address modified as configured, and changes are made to the IP and UDP checksums and decrements to the TTL field, as appropriate.

If the UDP-forwarding is used for BOOTP or DHCP forwarding purposes, do not configure or use the existing `bootprelay` function. However, if the previous `bootprelay` functions are adequate, you may continue to use them.



### NOTE

*UDP-forwarding only works across a layer 3 boundary.*

## Configuring UDP-Forwarding

To configure UDP-forwarding, the first thing you must do is create a UDP-forward destination profile. The profile describes the types of UDP packets (by port number) that are used, and where they are to be forwarded. You must give the profile a unique name, in the same manner as a VLAN, protocol filter, or Spanning Tree Domain.

Next, configure a VLAN to make use of the UDP-forwarding profile. As a result, all incoming traffic from the VLAN that matches the UDP profile is handled as specified in the UDP-forwarding profile.

A maximum of ten UDP-forwarding profiles can be defined. Each named profile may contain a maximum of eight “rules” defining the UDP port, and destination IP address or VLAN. A VLAN can make use of a single UDP-forwarding profile. UDP packets directed toward a VLAN use an all-ones broadcast on that VLAN.

## UDP-Forwarding Example

In this example, the *VLAN Marketing* and the *VLAN Operations* are pointed toward a specific backbone DHCP server (with IP address 10.1.1.1) and a backup server (with IP address 10.1.1.2). Additionally, the *VLAN LabUser* is configured to use any responding DHCP server on a separate VLAN called *LabSvrs*.

The commands for this configuration are as follows:

```
create udp-profile backbonedhcp
create udp-profile labdhcp
config backbonedhcp add 67 ipaddress 10.1.1.1
config backbonedhcp add 67 ipaddress 10.1.1.2
config labdhcp add 67 vlan labsvrs
config marketing udp-profile backbonedhcp
config operations udp-profile backbonedhcp
config labuser udp-profile labdhcp
```

## ICMP Packet Processing

As ICMP packets are routed or generated, you can take various actions to control distribution. For ICMP packets typically generated or observed as part of the routing function, you can assert control on a per-type, per-VLAN basis. You would alter the default settings for security reasons: to restrict the success of tools that can be used to find an important application, host, or topology information. The controls include the disabling of transmitting ICMP messages associated with unreachable, port-unreachables, time-exceeded, parameter-problems, redirects, time-stamp, and address-mask requests.

For ICMP packets that are typically routed, you can apply access lists to restrict forwarding behavior. Access lists are described in Chapter 10.

## UDP-Forwarding Commands

Table 61 describes the commands used to configure UDP-forwarding.

**Table 61:** UDP-Forwarding Commands

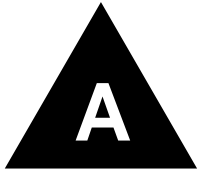
Command	Description
config udp-profile <profile_name> add <udp_port> [vlan <name>   ipaddress <dest_ipaddress>]	Adds a forwarding entry to the specified UDP-forwarding profile name. All broadcast packets sent to <udp_port> are forwarded to either the destination IP address (unicast or subnet directed broadcast) or to the specified VLAN as an all-ones broadcast.
config udp-profile <profile_name> delete <udp_port> [vlan <name>   ipaddress <dest_ipaddress>]	Deletes a forwarding entry from the specified udp-profile name.

**Table 61:** UDP-Forwarding Commands (continued)

Command	Description
config vlan <name> udp-profile <profile_name>	Assigns a UDP-forwarding profile to the source VLAN. Once the UDP profile is associated with the VLAN, the switch picks up any broadcast UDP packets that matches with the user configured UDP port number, and forwards those packets to the user-defined destination. If the UDP port is the DHCP/BOOTP port number, appropriate DHCP/BOOTP proxy functions are invoked.
create udp-profile <profile_name>	Creates a UDP-forwarding profile. You must use a unique name for the UDP-forwarding profile.
delete udp-profile <profile_name>	Deletes a UDP-forwarding profile.
show udp-profile {<profile_name>}	Displays the profile names, input rules of UDP port, destination IP address, or VLAN and the source VLANs to which the profile is applied.
unconfig udp-profile vlan [<name>   all]	Removes the UDP-forwarding profile configuration for one or all VLANs.







# Safety Information

---

## Important Safety Information



### WARNING!

---

***Read the following safety information thoroughly before installing your Extreme Networks switch. Failure to follow this safety information can lead to personal injury or damage to the equipment.***

Installation, maintenance, removal of parts, and removal of the unit and components must be done by qualified service personnel only.

Service personnel are people having appropriate technical training and experience necessary to be aware of the hazards to which they are exposed when performing a task and of measures to minimize the danger to themselves or other people.

Install the unit only in a temperature- and humidity-controlled indoor area free of airborne materials that can conduct electricity. Too much humidity can cause a fire. Too little humidity can produce electrical shock and fire.



### NOTE

---

*For more information about the Summit 300-48 temperature and humidity ranges, see Appendix B.*

## Power

The Summit 300-48 switch has two power inputs on the switch.

- The unit must be grounded. Do not connect the power supply unit to an AC outlet without a ground connection.
- The unit must be connected to a grounded outlet to comply with European safety standards.
- The socket outlet must be near the unit and easily accessible. You can only remove power from the unit by disconnecting the power cord from the outlet.
- This unit operates under Safety Extra Low Voltage (SELV) conditions according to IEC 950. The conditions are only maintained if the equipment to which it is connected also operates under SELV conditions.

- The appliance coupler (the connector to the unit and not the wall plug) must have a configuration for mating with an EN60320/IEC320 appliance inlet.
- *France and Peru only*  
This unit cannot be powered from IT<sup>†</sup> supplies. If your supplies are of IT type, this unit must be powered by 230 V (2P+T) via an isolation transformer ratio 1:1, with the secondary connection point labeled Neutral, connected directly to ground.

## Power Cord

The power cord must be approved for the country where it is used:

- USA and Canada
  - The cord set must be UL-listed and CSA-certified.
  - The minimum specification for the flexible cord is No. 18 AWG (1.5 mm<sup>2</sup>), Type SVT or SJT, 3-conductor.
  - The cord set must have a rated current capacity of at least the amount rated for each specific product.
  - The AC attachment plug must be an Earth-grounding type with a NEMA 5-15P (10 A, 125 V) configuration.
- Denmark
  - The supply plug must comply with section 107-2-D1, standard DK2-1a or DK2-5a.
- Switzerland
  - The supply plug must comply with SEV/ASE 1011.
- Argentina
  - The supply plug must comply with Argentinian standards.

## Connections

**Fiber Optic ports - Optical Safety.** Never look at the transmit LED/laser through a magnifying device while it is powered on. Never look directly at the fiber port or fiber cable ends when they are powered on.

This is a Class 1 laser device.



---

*Use only for data communications applications that require optical fiber. Use only with the appropriate connector. When not in use, replace dust cover. Using this module in ways other than those described in this manual can result in intense heat that can cause fire, property damage, or personal injury.*

## Lithium Battery

The lithium battery is not user-replaceable.



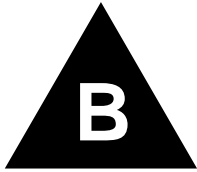
### WARNING!

---

*Danger of explosion if battery is incorrectly replaced. Replace only with the same or equivalent type recommended by the manufacturer. Dispose of used batteries according to the manufacturer's instructions.*

- Disposal requirements vary by country and by state.
- Lithium batteries are not listed by the Environmental Protection Agency (EPA) as a hazardous waste. Therefore, they can typically be disposed of as normal waste.
- If you are disposing of large quantities, contact a local waste-management service.
- No hazardous compounds are used within the battery module.
- The weight of the lithium contained in each coin cell is approximately 0.035 grams.
- Two types of batteries are used interchangeably:
  - CR chemistry uses manganese dioxide as the cathode material.
  - BR chemistry uses poly-carbonmonofluoride as the cathode material.





# Supported Standards

The following is a list of software standards supported by ExtremeWare for the Summit 300-48 switch.

---

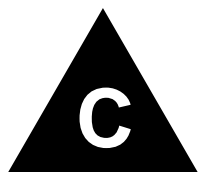
<b>Standards and Protocols</b>	
RFC 1122 Host requirements	RFC 793 TCP
IEEE 802.1D-1998 (802.1p) Packet priority	RFC 826 ARP
IEEE 802.1Q VLAN tagging	RFC 2068 HTTP
RFC 2474 DiffServ Precedence	RFC 2131 BootP/DHCP relay
RFC 783 TFTP	RFC 2030 - Simple Network Time Protocol
RFC 1542 BootP	RFC 1256 Router discovery protocol
RFC 854 Telnet	RFC 1812 IP router requirement
RFC 768 UDP	RFC 1519 CIDR
RFC 791 IP	
RFC 792 ICMP	

---

<b>Management and Security</b>	
RFC 1157 SNMP v1/v2c	RFC 2239 802.3 MAU MIB
RFC 1213 MIB II	802.11 MIB
RFC 1354 IP forwarding table MIB	ExtremeWare Enterprise MIB
RFC 1493 Bridge MIB	HTML and Telnet management
RFC 2037 Entity MIB	RFC 2138 RADIUS
RFC 1573 Evolution of Interface	RFC 2925 Ping MIB
RFC 1643 Ethernet MIB	RFC 2233 Interface MIB
RFC 1757 Four groups of RMON	RFC 2096 IP Forwarding Table MIB
ExtremeWare VLAN Configuration private MIB	999 local messages, criticals stored across reboots
RFC 2021 RMON probe configuration	

---





# Software Upgrade and Boot Options

---

This appendix describes the following topics:

- Downloading a New Image on page 175
- Saving Configuration Changes on page 176
- Using TFTP to Upload the Configuration on page 177
- Using TFTP to Download the Configuration on page 178
- Upgrading and Accessing BootROM on page 179
- Boot Option Commands on page 181

## Downloading a New Image

The image file contains the executable code that runs on the switch. It comes preinstalled from the factory. As new versions of the image are released, you should upgrade the software running on your system.

The image is upgraded by using a download procedure from either a Trivial File Transfer Protocol (TFTP) server on the network. Downloading a new image involves the following steps:

- Load the new image onto a TFTP server on your network (if you will be using TFTP).
- Download the new image to the switch using the following command:

```
download image [<ipaddress> | <hostname>] <filename> {primary | secondary}
```

where the following is true:

`ipaddress` — Is the IP address of the TFTP server.

`hostname` — Is the hostname of the TFTP server. (You must enable DNS to use this option.)

`filename` — Is the filename of the new image.

`primary` — Indicates the primary image.

`secondary` — Indicates the secondary image.

The switch can store up to two images; a primary and a secondary. When you download a new image, you must select into which image space (primary or secondary) the new image should be placed. If not indicated, the primary image space is used.

## Rebooting the Switch

To reboot the switch, use the following command:

```
reboot { time <date> <time> | cancel }
```

where `date` is the date and `time` is the time (using a 24-hour clock format) when the switch will be rebooted. The values use the following format:

```
mm/dd/yyyy hh:mm:ss
```

If you do not specify a reboot time, the reboot occurs immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the `cancel` option.

## Saving Configuration Changes

The configuration is the customized set of parameters that you have selected to run on the switch. As you make configuration changes, the new settings are stored in run-time memory. Settings that are stored in run-time memory are not retained by the switch when the switch is rebooted. To retain the settings, and have them load when you reboot the switch, you must save the configuration to nonvolatile storage.

The switch can store two different configurations: a primary and a secondary. When you save configuration changes, you can select to which configuration you want the changes saved. If you do not specify, the changes are saved to the configuration area currently in use.

If you have made a mistake, or you must revert to the configuration as it was before you started making changes, you can tell the switch to use the secondary configuration on the next reboot.

To save the configuration, use the following command:

```
save {configuration} {primary | secondary}
```

To use the configuration, use the following command:

```
use configuration [primary | secondary]
```

The configuration takes effect on the next reboot.



### NOTE

---

*If the switch is rebooted while in the middle of a configuration save, the switch boots to factory default settings. The configuration that is not in the process of being saved is unaffected.*

## Returning to Factory Defaults

To return the switch configuration to factory defaults, use the following command:

```
unconfig switch
```

This command resets the entire configuration, with the exception of user accounts and passwords that have been configured, and the date and time.



To erase the currently selected configuration image and reset all switch parameters, use the following command:

```
unconfig switch all
```

## Using TFTP to Upload the Configuration

You can upload the current configuration to a TFTP server on your network. The uploaded ASCII file retains the command-line interface (CLI) format. This allows you to:

- Modify the configuration using a text editor, and later download a copy of the file to the same switch, or to one or more different switches.
- Send a copy of the configuration file to the Extreme Networks Technical Support department for problem-solving purposes.
- Automatically upload the configuration file every day, so that the TFTP server can archive the configuration on a daily basis. Because the filename is not changed, the configured file stored in the TFTP server is overwritten every day.

To upload the configuration, use the following command:

```
upload configuration [<ipaddress> | <hostname>] <filename> {every <time>}
```

where the following is true:

- `ipaddress` — Is the IP address of the TFTP server.
- `hostname` — Is the hostname of the TFTP server. (You must enable DNS to use this option.)
- `filename` — Is the name of the ASCII file. The filename can be up to 255 characters long, and cannot include any spaces, commas, quotation marks, or special characters.
- `every <time>` — Specifies the time of day you want the configuration automatically uploaded on a daily basis. If not specified, the current configuration is immediately uploaded to the TFTP server.

To cancel a previously scheduled configuration upload, use the following command:

```
upload configuration cancel
```

## Using TFTP to Download the Configuration

You can download ASCII files that contain CLI commands to the switch to modify the switch configuration. Three types of configuration scenarios that can be downloaded:

- Complete configuration
- Incremental configuration
- Scheduled incremental configuration

### Downloading a Complete Configuration

Downloading a complete configuration replicates or restores the entire configuration to the switch. You typically use this type of download in conjunction with the `upload config` command, which generates a complete switch configuration in an ASCII format. As part of the complete configuration download, the switch is automatically rebooted.

To download a complete configuration, use the following command:

```
download configuration [<hostname> | <ipaddress>] <filename>
```

After the ASCII configuration is downloaded by way of TFTP, you are prompted to reboot the switch. The downloaded configuration file is stored in current switch memory during the rebooting process, and is not retained if the switch has a power failure.

When the switch completes booting, it treats the downloaded configuration file as a script of CLI commands, and automatically executes the commands. If your CLI connection is through a Telnet connection (and not the console port), your connection is terminated when the switch reboots, but the command executes normally.

### Downloading an Incremental Configuration

A partial or incremental change to the switch configuration may be accomplished by downloaded ASCII files that contain CLI commands. These commands are interpreted as a script of CLI commands, and take effect at the time of the download, without requiring a reboot of the switch.

To download an incremental configuration, use the following command:

```
download configuration [<hostname> | <ipaddress>] <filename> {incremental}
```

### Scheduled Incremental Configuration Download

You can schedule the switch to download a partial or incremental configuration on a regular basis. You could use this feature to update the configuration of the switch regularly from a centrally administered TFTP server. As part of the scheduled incremental download, you can optionally configuration a backup TFTP server.

To configure the primary and/or secondary TFTP server and filename, use the following command:

```
config download server [primary | secondary] [<hostname> | <ipaddress>] <filename>
```

To enable scheduled incremental downloads, use the following command:

```
download configuration every <hour (0-23)>
```

To display scheduled download information, use the following command:

```
show switch
```

To cancel scheduled incremental downloads, use the following command:

```
download configuration cancel
```

## Remember to Save

Regardless of which download option is used, configurations are downloaded into switch runtime memory, only. The configuration is saved only when the `save` command is issued, or if the configuration file, itself, contains the `save` command.

If the configuration currently running in the switch does not match the configuration that the switch used when it originally booted, an asterisk (\*) appears before the command line prompt when using the CLI.

## Upgrading and Accessing BootROM

The Summit 300-48 switch has a two-stage BootROM. The first stage, called bootstrap, does basic initialization of the switch processor and will load one of two second-stage bootloaders (called primary and secondary).

In the event the switch does not boot properly, both bootstrap and bootloader will allow the user to access the boot options using the CLI.

If necessary, the bootloader can be updated, after the switch has booted, using TFTP.

### Upgrading Bootloader

Upgrading Bootloader is done using TFTP (from the CLI), after the switch has booted. Upgrade the BootROM only when asked to do so by an Extreme Networks technical representative. To upgrade the BootROM, use the following command:

```
download bootrom [<hostname> | <ipaddress>] <filename> [ bootstrap | diagnostics |
primary_bootloader | secondary_bootloader]
```

### Accessing the Bootstrap CLI

The Bootstrap CLI contains commands to support the selection of which bootloader to use.

To access the Bootstrap CLI, follow these steps:

- 1 Attach a serial cable to the serial console port of the switch.
- 2 Attach the other end of the serial cable to a properly configured terminal or terminal emulator.
- 3 Power cycle or reboot the switch.
- 4 As soon as you see the Bootstrap Banner, press the spacebar.

The `BOOTSTRAP>` prompt will appear on the screen.

Table 64 lists the Bootstrap commands.

**Table 62:** Bootstrap Command Options

Option	Description
boot	Boots a loader.
enable	Enables features.
h	Accesses online help.
help	Accesses online help.
?	Accesses online help.
reboot	Reboots the system.
rz	zmodem download.
show	Displays bootstrap information.
use	Sets the file to use for config, loader and image commands.

## Accessing the Bootloader CLI

The Bootloader CLI contains commands that support the selection of image and configuration for the switch.

To access the Bootloader CLI, follow these steps:

- 1 Attach a serial cable to the serial console port of the switch.
- 2 Attach the other end of the serial cable to a properly configured terminal or terminal emulator.
- 3 Power cycle or reboot the switch.
- 4 As soon as you see the Bootloader Banner, press the spacebar.

The `BOOTLOADER>` prompt will appear on the screen.

Table 64 lists the Bootloader commands.


**Table 63:** Bootloader Command Options

Option	Description
boot	Boots an image.
enable	Enables features.
h	Accesses online help.
help	Accesses online help.
?	Accesses online help.
reboot	Reboots the system.
hi	Displays command history.
show	Displays bootstrap information.
cd	Changes working CF directory.
pwd	Prints working CF directory.

# Boot Option Commands

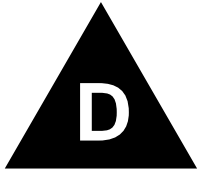
Table 64 lists the CLI commands associated with switch boot options.

**Table 64:** Boot Option Commands

Command	Description
config download server [primary   secondary] [-hostname>   <ipaddress>] <filename>	Configures the TFTP server(s) used by a scheduled incremental configuration download.
download bootrom [<hostname>   <ipaddress>] <filename> [bootstrap   diagnostics   primary_bootloader   secondary_bootloader]	Downloads a BOOT ROM image from a TFTP server. The downloaded image replaces the BOOT ROM in the onboard FLASH memory.
 <b>NOTE</b>	
	<i>If this command does not complete successfully, it could prevent the switch from booting.</i>
download configuration [<hostname>   <ipaddress>] <filename> {incremental}	Downloads a complete configuration. Use the <code>incremental</code> keyword to specify an incremental configuration download.
download configuration cancel	Cancels a previously scheduled configuration download.
download configuration every <hour>	Schedules a configuration download. Specify the hour using a 24-hour clock, where the range is 0 to 23.
download image [<ipaddress>   <hostname>] <filename> {primary   secondary}	Downloads a new image from a TFTP server over the network. If no parameters are specified, the image is saved to the current image.
reboot {time <date> <time>   cancel}	Reboots the switch at the date and time specified. If you do not specify a reboot time, the reboot happens immediately following the command, and any previously scheduled reboots are cancelled. To cancel a previously scheduled reboot, use the <code>cancel</code> option.
save {configuration} {primary   secondary}	Saves the current configuration to nonvolatile storage. You can specify the primary or secondary configuration area. If not specified, the configuration is saved to the primary configuration area.
show configuration	Displays the current configuration to the terminal. You can then capture the output and store it as a file.
upload configuration [<ipaddress>   <hostname>] <filename> {every <time>}	Uploads the current run-time configuration to the specified TFTP server. If <code>every &lt;time&gt;</code> is specified, the switch automatically saves the configuration to the server once per day, at the specified time. If the time option is not specified, the current configuration is immediately uploaded.
upload configuration cancel	Cancels a previously schedule configuration upload.

**Table 64:** Boot Option Commands (continued)

<b>Command</b>	<b>Description</b>
use configuration [primary   secondary]	Configures the switch to use a particular configuration on the next reboot. Options include the primary configuration area or the secondary configuration area.
use image [primary   secondary]	Configures the switch to use a particular image on the next reboot.



# Troubleshooting

---

If you encounter problems when using the switch, this appendix may be helpful. If you have a problem not listed here or in the release notes, contact your local technical support representative.

## LEDs

### **Power LED does not light:**

Check that the power cable is firmly connected to the device and to the supply outlet.

### **On powering-up, the MGMT LED lights yellow:**

The device has failed its Power On Self Test (POST) and you should contact your supplier for advice.

### **A link is connected, but the Port Status LED does not light:**

Check that:

- All connections are secure.
- Cables are free from damage.
- The devices at both ends of the link are powered-up.

- Both ends of the Gigabit link are set to the same autonegotiation state.

Both sides of the Gigabit link must be enabled or disabled. If the two are different, typically the side with autonegotiation disabled will have the link LED lit, and the side with autonegotiation enabled will not be lit. The default configuration for a Gigabit port is autonegotiation enabled. This can be verified by entering the following command:

```
show port config
```

**Switch does not power up:**

All products manufactured by Extreme Networks use digital power supplies with surge protection. In the event of a power surge, the protection circuits shut down the power supply. To reset, unplug the switch for 1 minute, plug it back in, and attempt to power up the switch.

If this does not work, try using a different power source (different power strip/outlet) and power cord.

## Using the Command-Line Interface

**The initial welcome prompt does not display:**

Check that your terminal or terminal emulator is correctly configured.

For console port access, you may need to press [Return] several times before the welcome prompt appears.

Check the settings on your terminal or terminal emulator. The settings are 9600 baud, 8 data bits, 1 stop bit, no parity, no flow control.

**The SNMP Network Manager cannot access the device:**

Check that the device IP address, subnet mask, and default router are correctly configured, and that the device has been reset.

Check that the device IP address is correctly recorded by the SNMP Network Manager (refer to the user documentation for the Network Manager).

Check that the community strings configured for the system and Network Manager are the same.

Check that SNMP access was not disabled for the system.

**The Telnet workstation cannot access the device:**

Check that the device IP address, subnet mask and default router are correctly configured, and that the device has been reset. Ensure that you enter the IP address of the switch correctly when invoking the Telnet facility. Check that Telnet access was not disabled for the switch. If you attempt to log in and the maximum number of Telnet sessions are being used, you should receive an error message indicating so.

**Traps are not received by the SNMP Network Manager:**

Check that the SNMP Network Manager's IP address and community string are correctly configured, and that the IP address of the Trap Receiver is configured properly on the system.

**The SNMP Network Manager or Telnet workstation can no longer access the device:**

Check that Telnet access or SNMP access is enabled.



Check that the port through which you are trying to access the device has not been disabled. If it is enabled, check the connections and network cabling at the port.

Check that the port through which you are trying to access the device is in a correctly configured VLAN.

Try accessing the device through a different port. If you can now access the device, a problem with the original port is indicated. Re-examine the connections and cabling.

A network problem may be preventing you accessing the device over the network. Try accessing the device through the console port.

Check that the community strings configured for the device and the Network Manager are the same.

Check that SNMP access was not disabled for the system.

#### **Permanent entries remain in the FDB:**

If you have made a permanent entry in the FDB (which requires you to specify the VLAN to which it belongs and then delete the VLAN), the FDB entry will remain. Though causing no harm, you must manually delete the entry from the FDB if you want to remove it.

#### **Default and Static Routes:**

If you have defined static or default routes, those routes will remain in the configuration independent of whether the VLAN and VLAN IP address that used them remains. You should manually delete the routes if no VLAN IP address is capable of using them.

#### **You forget your password and cannot log in:**

If you are not an administrator, another user having administrator access level can log in, delete your user name, and create a new user name for you, with a new password.

Alternatively, another user having administrator access level can log in and initialize the device. This will return all configuration information (including passwords) to the initial values.

In the case where no one knows a password for an administrator level user, contact your supplier.

## **Port Configuration**

#### **No link light on 10/100 Base port:**

If patching from a hub or switch to another hub or switch, ensure that you are using a CAT5 cross-over cable. This is a CAT5 cable that has pins 1&2 on one end connected to pins 3&6 on the other end.

#### **Excessive RX CRC errors:**

When a device that has auto-negotiation disabled is connected to a Extreme switch that has auto-negotiation enabled, the Extreme switch links at the correct speed, but in half duplex mode. The Extreme switch 10/100 physical interface uses a method called *parallel detection* to bring up the link. Because the other network device is not participating in auto-negotiation (and does not advertise its capabilities), parallel detection on the Extreme switch is only able to sense 10Mbps versus 100Mbps speed, and not the duplex mode. Therefore, the switch establishes the link in half duplex mode using the correct speed.

The only way to establish a full duplex link is to either force it at both sides, or run auto-negotiation on both sides (using full duplex as an advertised capability, which is the default setting on the Extreme switch).

**NOTE**

*A mismatch of duplex mode between the Extreme switch and another network device will cause poor network performance. Viewing statistics using the `show port rx` command on the Extreme switch may display a constant increment of CRC errors. This is characteristic of a duplex mismatch between devices. This is NOT a problem with the Extreme switch.*

Always verify that the Extreme switch and the network device match in configuration for speed and duplex.

**No link light on Gigabit fiber port:**

Check to ensure that the transmit fiber goes to the receive fiber side of the other device, and vice-versa. All gigabit fiber cables are of the cross-over type.

The Extreme switch has auto-negotiation set to on by default for gigabit ports. These ports need to be set to auto off (using the command `config port <port #> auto off`) if you are connecting it to devices that do not support auto-negotiation.

Ensure that you are using multi-mode fiber (MMF) when using a 1000BASE-SX Mini-GBIC. 1000BASE-SX does not work with single-mode fiber (SMF).

## VLANs

**You cannot add a port to a VLAN:**

If you attempt to add a port to the “default” VLAN and get an error message similar to

```
Summit 300-48:28 # config vlan default add port 1:1
ERROR: There is a protocol conflict with adding port 1:1 untagged to VLAN default
```

you already have a VLAN using untagged traffic on this port. Only one VLAN using untagged traffic can be configured on a single physical port.

VLAN configuration can be verified by using the following command:

```
show vlan <name>
```

The solution for this error is to remove port 1 from the VLAN currently using untagged traffic on the port. If this were the “default” VLAN, the command would be

```
Summit 300-48:30 # config vlan default del port 1:1
```

which should now allow you to re-enter the previous command without error as follows:

```
Summit 300-48:31 # config vlan red add port 1:1
```

**VLAN names:**

There are restrictions on VLAN names. They cannot contain whitespaces and cannot start with a numeric value unless you use quotation marks around the name. If a name contains whitespaces, starts

with a number, or contains non-alphabetical characters, you must use quotation marks whenever referring to the VLAN name.

### **VLANs, IP Addresses and default routes:**

The system can have an IP address for each configured VLAN. It is necessary to have an IP address associated with a VLAN if you intend to manage (Telnet, SNMP, ping) through that VLAN or route IP traffic. You can also configure multiple default routes for the system. The system first tries the default route with the lowest cost metric.

## **STP**

### **You have connected an endstation directly to the switch and the endstation fails to boot correctly:**

The switch has STP enabled, and the endstation is booting before the STP initialization process is complete. Specify that STP has been disabled for that VLAN, or turn off STP for the switch ports of the endstation and devices to which it is attempting to connect, and then reboot the endstation.

### **The switch keeps aging out endstation entries in the switch Forwarding Database (FDB):**

Reduce the number of topology changes by disabling STP on those systems that do not use redundant paths.

Specify that the endstation entries are static or permanent.

## Debug Tracing

ExtremeWare includes a debug-tracing facility for the switch. The show debug-tracing command can be applied to one or all VLANs, as follows:

```
show debug-tracing {vlan <name>}
```

The debug commands should only be used under the guidance of Extreme Networks technical personnel.

## TOP Command

The top command is a utility that indicates CPU utilization by process.

## Contacting Extreme Technical Support

If you have a network issue that you are unable to resolve, contact Extreme Networks technical support. Extreme Networks maintains several Technical Assistance Centers (TACs) around the world to answer networking questions and resolve network problems. You can contact technical support by phone at:

- (800) 998-2408
- (408) 579-2826

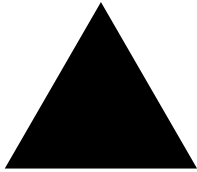
or by email at:

- [support@extremenetworks.com](mailto:support@extremenetworks.com)

You can also visit the support website at:

- <http://www.extremenetworks.com/extreme/support/techsupport.asp>

to download software updates (requires a service contract) and documentation.



# Index

## Numerics

02.1x/EAP	84
802.11a, 802.11b, 802.11g	74
802.1p configuration commands (table)	127

## A

access control lists	
description	107
examples	116
ICMP filter example	119
verifying settings	112
access levels	28
access lists	
adding	111
configuration commands (table)	113
deleting	112
permit-established example	116
permit-established keyword	111
access masks	
adding	111
deleting	112
access policies, description	107
access profiles	
ExtremeWare Vista	47
accounts	
creating	30
deleting	31
viewing	31
adding	
access lists	111
access masks	111
rate limits	111
Address Resolution Protocol. <i>See</i> ARP	
admin account	29
aging entries, FDB	103
alarm actions	144
Alarms, RMON	143
ARP	
clearing entries	163
communicating with devices outside subnet	156
configuring proxy ARP	156
incapable device	156
proxy ARP between subnets	156
proxy ARP, description of	156
responding to ARP requests	156
table, displaying	158

authentication	84
authentication method	
802.1x/EAP	84
WEP	84
autonegotiation	56

## B

blackhole entries, FDB	104
boot option commands (table)	181
Bootloader	
upgrading	179
BOOTP	
and UDP-Forwarding	165
BOOTP relay	
configuring	164
BOOTP, using	36
bootstrap command options (table)	180
BPDU tunneling	146
bridging	75
browser	
controls	49
fonts	48
setting up	47

## C

cipher suites	85
CLI	
command history	26
command shortcuts	24
line-editing keys	25
named components	25
numerical ranges, Summit 300-48 switch	24
symbols	25
syntax helper	24
using	
client configuration commands	80
command	
history	26
shortcuts	24
syntax, understanding	23
Command-Line Interface. <i>See</i> CLI	
common commands (table)	26
common power pool	97
communicating with devices outside subnet	156
complete configuration download	178

configuration			
downloading	178	factory defaults	20
downloading complete	178	features	17
downloading incremental	178	ExtremeWare Vista	
logging	140	accessing	48
primary and secondary	176	browser controls	49
saving changes	176	browser setup	47
schedule download	178	capturing screen output	51
uploading to file	177	controlling access	47
wireless ports	79	fonts	48
configuring PoE	98	home page	47, 48
console connection	36	navigating	48
controlling Telnet access	39	saving changes	50
conventions		screen layout	48
notice icons, About This Guide	15	screen resolution	48
text, About This Guide	16	status messages	50
creating		VLAN configuration	47
access lists	111		
access masks	111	<b>F</b>	
rate limits	111	FDB	
		adding an entry	104
<b>D</b>		aging entries	103
database applications, and QoS	122	blackhole entries	104
default		configuration commands (table)	105
passwords	30	configuring	105
settings	20	contents	103
users	29	creating a permanent entry example	106
default STP domain	146	displaying	106
default VLAN	69	dynamic entries	103
delete		entries	103
access list	112	non-aging entries	103
access masks	112	permanent entries	103
rate limit	112	QoS profile association	104
deleting a session	38	feature licensing	
DHCP and UDP-Forwarding	165	description	19
DHCP relay, configuring	164	file server applications, and QoS	123
DiffServ, configuring	128	fonts, browser	48
disabling a switch port	55	Forwarding Database. <i>See</i> FDB	
disconnecting a Telnet session	38		
DNS		<b>G</b>	
configuration commands (table)	31	Greenwich Mean Time Offsets (table)	52
description	31		
Domain Name Service. <i>See</i> DNS		<b>H</b>	
domains, Spanning Tree Protocol	145	History, RMON	143
downloading incremental configuration	178	home page	47, 48
dynamic entries, FDB	103		
		<b>I</b>	
<b>E</b>		ICMP configuration commands (table)	160
EAP-MD5	74	IEEE 802.1Q	66
EAP-TLS	74	image	
EAP-TLS (Transport Layer Security)	85	downloading	175
EAP-TTLS	74	primary and secondary	175
EAP-TTLS (Tunneled TLS)	85	upgrading	175
EDP		interfaces, router	154
commands (table)	61	IP address, entering	37
description	61	IP route sharing	155
enabling a switch port	55	IP TOS configuration commands (table)	128
errors, port	136	IP unicast routing	
establishing a Telnet session	36	basic IP commands (table)	158
Events, RMON	143	BOOTP relay	164
export restrictions	20	configuration examples	162
Extreme Discovery Protocol <i>See</i> EDP		configuring	157
ExtremeWare		default gateway	153

DHCP relay	164	<b>N</b>	
disabling	163	names, VLANs	69
enabling	157	network security policies	87
IP route sharing	155	non-aging entries, FDB	103
proxy ARP	156		
reset and disable commands (table)	163	<b>O</b>	
resetting	163	opening a Telnet session	36
router interfaces	154		
router show commands (table)	163	<b>P</b>	
routing table		passwords	
configuration commands (table)	159	default	30
multiple routes	155	forgetting	30
populating	154	PEAP	74
static routes	155	PEAP (protected EAP)	85
settings, displaying	163	permanent entries, FDB	103
verifying the configuration	158	permit-established keyword	111
IRDP	162	ping command	32
<b>K</b>		PoE	95
keys		configuring	98
line-editing	25	LEDs for usage	98
port monitoring	137	PoE features	95
<b>L</b>		port	
LEDs for PoE usage	98	autonegotiation	56
licensing		configuring on Summit 300-48 switch	55
description	19	enabling and disabling	55
line-editing keys	25	errors, viewing	136
load sharing		monitoring display keys	137
algorithms	57	personality	74
configuring	58	priority, STP	149
description	57	receive errors	136
load-sharing group, description	57	statistics, viewing	135
master port	58	STP state, displaying	151
verifying the configuration	59	STPD membership	146
local logging	139	Summit24e3 switch	55
location-based authentication	85	switch commands (table)	56
log display	139	transmit errors	136
logging		port connection order	97
and Telnet	139	port numbering	55
commands (table)	140	port power management	96
configuration changes	140	port power operator limit	96
description	138	port power priorities	97
fault level	138	port power reset	97
local	139	port-based VLANs	64
message	139	port-mirroring	
real-time display	139	and protocol analyzers	60
remote	139	description	59
subsystem	138	example	61
timestamp	138	switch configuration commands (table)	60
logging in	30	ports	
<b>M</b>		wireless interfaces	75
MAC-based VLANs	75	power	
management access	28	budget management	96
master port		common pool	97
load sharing	58	consuming more than allocated	98
maximum Telnet session	36	operator limit	96
MIBs	41	port	96
mirroring. <i>See</i> port-mirroring		port connection order	97
monitoring the switch	133	port priorities	97
multiple routes	155	port reset	97
		power events	97
		reserved	96
		power events	97
		power over Ethernet	95

primary image	175	deleting	112
privacy	85	rate-limiting	132
<i>private</i> community, SNMP	41	receive errors	136
protocol analyzers, use with port-mirroring	60	remote logging	139
proxy ARP		Remote Monitoring. <i>See</i> RMON	
communicating with devices outside subnet	156	renaming a VLAN	70
conditions	156	reserved power	96
configuring	156	reset to factory defaults	176
MAC address in response	156	responding to ARP requests	156
responding to requests	156	RF configuration commands	76
subnets	156	RF properties	76
table, displaying	163	RF property values	76
proxy ARP, description	156	RMON	
<i>public</i> community, SNMP	41	alarm actions	144
		Alarms group	143
		Events group	143
		features supported	142
		History group	143
		probe	142
		Statistics group	142
		route sharing. <i>See</i> IP route sharing	
		router interfaces	154
		routing table, populating	154
		routing. <i>See</i> IP unicast routing	
		RSN support	86
<b>Q</b>		<b>S</b>	
QoS		safety information	169
802.1p configuration commands (table)	127	saving changes using ExtremeWare Vista	50
802.1p priority	126	saving configuration changes	176
applications	122	scheduling configuration download	178
blackhole	125	screen resolution, ExtremeWare Vista	48
configuration commands (table)	123	secondary image	175
database applications	122	security	83
description	18, 121	security capabilities	83
DiffServ, configuring	128	security commands	89
examples		security licensing	
MAC address	125	description	20
source port	130	obtaining	20
VLAN	130	security policies	87
FDB entry association	104	and RADIUS support	88
file server applications	123	security policy design	87
IP TOS configuration commands (table)	128	security policy examples	88
traffic groupings	124	sessions, deleting	38
access list	124	shortcuts, command	24
blackhole	125	Simple Network Management Protocol. <i>See</i> SNMP	
explicit packet marking	126	SNMP	
MAC address	125	community strings	41
source port	130	configuration commands (table)	41
VLAN	130	configuring	41
traffic groupings (table)	124	settings, displaying	42
verifying	132	supported MIBs	41
video applications	122	system contact	41
voice applications	122	system location	41
web browsing applications	123	system name	41
QoS monitor		trap receivers	41
description	131	using	40
real-time display	131	SNTP	
Quality of Service. <i>See</i> QoS	121	configuration commands (table)	54
		configuring	51
		Daylight Savings Time	51
		description	51
		example	54
		Greenwich Mean Time offset	51
<b>R</b>			
RADIUS			
client configuration	43		
configuration commands (table)	43		
description	43		
Merit server configuration (example)	44		
per-command configuration (example)	45		
RFC 2138 attributes	44		
servers	43		
TCP port	43		
RADIUS attributes			
wireless	88		
rate limits			
adding	111		

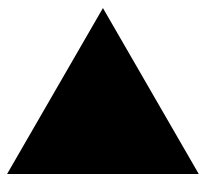


Greenwich Mean Time Offsets (table)	52	controlling access	39
NTP servers	51	disconnecting a session	38
software licensing		logging	139
security features	20	maximum sessions	36
SSH2 protocol	20	opening a session	36
Spanning Tree Protocol. <i>See</i> STP		using	36
speed, ports	56	TFTP	
SSH2 protocol		server	175
authentication key	40	using	177
description	20, 39	time-Based Authentication	85
enabling	39	TKIP	74
predefined clients	40	traceroute command	32
TCP port number	40	traffic groupings	124
stand-alone switch		traffic rate-limiting	132
enabling and disabling ports	55	transmit errors	136
static routes	155	transmit queues	75
statistics		trunks	67
port	135		
Statistics, RMON	142	<b>U</b>	
status monitoring	133	UDP-Forwarding	
status monitoring commands (table)	134	and BOOTP	165
STP		and DHCP	165
and VLANs	146	configuration commands (table)	166
BPDU tunneling	146	configuring	165
bridge priority	149	description	165
configurable parameters	149	example	166
configuration commands (table)	149	profiles	165
configuration example	151	VLANs	165
configuring	148	unified access security	83
default domain	146	upgrading the image	175
description	18	uploading the configuration	177
disable and reset commands (table)	152	user access security	84
displaying settings	151	user account	29
domains	145	users	
examples	146	access levels	28
forward delay	149	authenticating	43
hello time	149	creating	30
max age	149	default	29
overview	145	viewing	31
path cost	149		
port priority	149	<b>V</b>	
port state, displaying	151	video applications, and QoS	122
Summit 300-48 switch		viewing accounts	31
load sharing	58	Virtual LANs. <i>See</i> VLANs	
port configuration	55	VLAN tagging	66
Summit24e3 switch		VLANs	
load sharing example	59	and ExtremeWare Vista	47
verifying load sharing	59	and STP	146
switch		assigning a tag	67
logging	138	benefits	63
monitoring	133	configuration commands (table)	70
RMON features	142	configuration examples	71
switch port commands (table)	56	configuring	70
syntax, understanding	23	<i>default</i>	69
syslog host	139	description	18
system contact, SNMP	41	displaying settings	71
system location, SNMP	41	mixing port-based and tagged	69
system name, SNMP	41	names	69
		port-based	64
<b>T</b>		renaming	70
tagging, VLAN	66	routing	157
technical support	187	tagged	66
Telnet		trunks	67
connecting to another host	36		

types	64
UDP-Forwarding	165
voice applications, QoS	122

## W

Web access, controlling	47
web browsing applications, and QoS	123
WEP	84
wireless	
event logging and reporting	81
example network	74
features	74
networking	73
show commands	80
wireless ports	
configuration commands	80
configuration process	75
configuring	79
interfaces	75
managing	75
WPA	74



# Index of Commands

## C

clear counters	140	config log display	139, 140
clear fdb	105, 125	config mirroring add	60
clear inline-power connection-history slot	99	config mirroring delete	60
clear inline-power fault ports	100	config ports auto off	26, 56
clear iparp	158, 163	config ports auto on	56
clear ipfdb	158, 163	config ports display-string	56
clear log	140	config ports qosprofile	123, 130
clear session	26, 38	config radius server	43
config account	26	config radius shared-secret	43
config banner	26	config rf-profile	76
config bootprelay add	158, 165	config security-profile	89
config bootprelay delete	158, 165	config sharing address-based	56, 58
config dns-client add	31	config snmp add trapreceiver	41
config dns-client default-domain	31	config snmp community	41
config dns-client delete	31	config snmp delete trapreceiver	41
config download server	178, 181	config snmp syscontact	41
config fdb agingtime	105	config snmp syslocation	41
config inline-power budget	99	config snmp sysname	42
config inline-power detection	100	config snmp-client	52
config inline-power disconnect-precedence	99	config snmp-client server	54
config inline-power operator-limit	99	config snmp-client update-interval	52, 54
config inline-power priority	101	config ssh2 key	26, 40
config inline-power reserved-budget	100	config ssh2 key pregenerated	40
config inline-power usage-threshold	99	config stpd add vlan	148, 149
config inline-power violation-precedence	100	config stpd forwarddelay	149
config iparp add	158	config stpd hellotime	149
config iparp add proxy	156, 158	config stpd maxage	150
config iparp delete	158	config stpd port cost	150
config iparp delete proxy	158	config stpd port priority	150
config iparp timeout	158	config stpd priority	150
config iproute add	159	config syslog	139, 141
config iproute add blackhole	159	config syslog delete	141
config iproute add default	38, 157, 160	config sys-recovery-level	27, 137
config iproute delete	160	config time	27
config iproute delete blackhole	160	config timezone	27, 51
config iproute delete default	160	config udp-profile add	166
config iproute delete blackhole	160	config udp-profile delete	166
config iproute delete default	160	config vlan add port	70
config iproute priority	157, 160	config vlan delete port	70
config irdp	160		

config vlan ipaddress	27, 38, 70, 157	disable inline-power ports	99
config vlan name	70	disable inline-power slot	98
config vlan priority	127	disable ipforwarding	159, 164
config vlan qosprofile	123, 130	disable ipforwarding broadcast	159, 164
config vlan tag	70	disable ip-option loose-source-route	161
config vlan udp-profile	167	disable ip-option record-route	161
config wireless port	79	disable ip-option record-timestamp	161
config wireless port interface	80	disable ip-option strict-source-route	161
configure wireless	78	disable ip-option use-router-alert	161
create access-list	111, 113	disable iproute sharing	160
create access-mask	111, 114	disable irdp	164
create account	27, 30	disable learning port	105
create fdbentry	105, 125	disable log display	141
create fdbentry blackhole	105	disable loopback-mode vlan	159
create fdbentry dynamic	105	disable mirroring	60
create rate-limit	111, 115	disable ports	27, 55, 56
create rf-profile copy	76	disable rmon	143
create rf-profile mode	76	disable sharing	56, 59
create security-profile	89	disable snmp access	42
create stpd	148, 150	disable snmp traps	42
create udp-profile	167	disable sntp-client	54
create vlan	27, 70	disable ssh2	28
<b>D</b>			
delete access-list	112, 115	disable stpd	152
delete access-mask	112, 116	disable stpd port	152
delete account	27	disable syslog	141
delete fdbentry	105	disable telnet	28, 39
delete rate-limit	112, 116	disable web	47
delete rf-profile	76	disable wireless ports	79
delete security-profile	89	download bootrom	31, 181
delete stpd	152	download configuration	31, 178, 181
delete udp-profile	167	download configuration cancel	179, 181
delete vlan	27, 71	download configuration every	178, 181
disable bootp	27, 159, 163	download configuration incremental	178
disable bootprelay	159, 163	download image	31, 175, 181
disable cli-config-logging	27, 140, 141	<b>E</b>	
disable clipaging	27	enable bootp	28, 159
disable diffserv examination ports	128	enable bootp vlan	37
disable edp ports	61	enable bootprelay	37, 159, 164
disable icmp	164	enable cli-config-logging	28, 140, 141
disable icmp address-mask	164	enable clipaging	28
disable icmp parameter-problem	160	enable diffserv examination ports	128, 129
disable icmp port-unreachables	164	enable edp ports	61
disable icmp redirects	164	enable icmp address-mask	161
disable icmp time-exceeded	164	enable icmp parameter-problem	161
disable icmp timestamp	164	enable icmp redirects	161
disable icmp unreachable	164	enable icmp time-exceeded	161
disable icmp userredirects	164	enable icmp timestamp	161
disable idletimeouts	27	enable icmp unreachable	161
disable ignore-bpdu	146	enable icmp userredirects	161
disable ignore-bpdu vlan	152	enable idletimeouts	28
disable ignore-stp vlan	152	enable ignore-bpdu	146
disable inline-power	98	enable ignore-bpdu vlan	150
		enable ignore-stp vlan	150

enable inline-power	98
enable inline-power ports	99
enable inline-power slot	98
enable ipforwarding	157, 159
enable ipforwarding broadcast	159
enable ip-option loose-source-route	161
enable ip-option record-route	161
enable ip-option record-timestamp	161
enable ip-option strict-source-route	161
enable ip-option use-router-alert	162
enable iproute sharing	160
enable irdp	162
enable learning port	106
enable log display	139, 141
enable loopback-mode vlan	159
enable mirroring	60
enable ports	55, 56
enable rmon	143
enable route sharing	155
enable sharing	57, 59
enable snmp access	42
enable snmp traps	42
enable sntp-client	51, 54
enable ssh2	28, 39
enable stpd	149, 150
enable stpd port	150
enable syslog	139, 141
enable telnet	28, 39
enable web	47
enable wireless ports	79

## H

history	26, 28
---------	--------

## L

logout	38
--------	----

## N

nslookup	31
----------	----

## P

ping	31, 32
------	--------

## Q

quit	38
------	----

## R

reboot	176, 181
reset inline-power ports	100
reset wireless ports	79
restart ports	57
rtlookup	160

## S

save	38, 176, 181
show access-list	112, 116
show access-mask	112, 116
show accounts	31
show banner	28
show configuration	181
show debug-tracing	187
show dns-client	31
show edp	61
show fdb	106
show fdb permanent	125, 132
show inline-power	101
show inline-power configuration port	101
show inline-power configuration slot	101
show inline-power info	101
show inline-power slot	101
show inline-power stats port	101
show inline-power stats slot	101
show iparp	158, 163
show iparp proxy	163
show ipconfig	158, 163, 165
show ipfdb	158, 163
show iproute	158
show ipstats	163
show log	134, 139, 141
show log config	134, 141
show management	39, 42, 47
show memory	134
show mirroring	60
show ports collisions	57
show ports configuration	57, 59
show ports info	57, 129, 131, 132
show ports packet	57
show ports qosmonitor	131
show ports rxerrors	57, 136
show ports stats	57, 135
show ports txerrors	57, 136
show ports utilization	57
show qosprofile	125, 130, 132
show radius	44
show rate-limit	112, 116
show security-profile	89
show session	38
show sharing address-based	57, 58
show sntp client	52
show sntp-client	54
show stpd	151
show stpd port	151
show switch	52, 132, 134, 179
show tech-support	135
show udp-profile	167
show version	135
show vlan	71, 131, 132

show wireless config	80
show wireless ports	80
show wireless ports interface	80

## T

telnet	31, 36
traceroute	31, 32

## U

unconfig icmp	162, 164
unconfig inline-power detection ports	100
unconfig inline-power disconnect-precedence	100
unconfig inline-power operator-limit ports	101
unconfig inline-power reserved-budget ports	101
unconfig inline-power usage-threshold	99
unconfig inline-power violation-precedence ports	101
unconfig irdp	162, 164
unconfig management	42
unconfig ports display-string	57
unconfig ports monitor vlan	71
unconfig radius	44
unconfig stpd	152
unconfig switch	28, 176
unconfig switch all	177
unconfig udp-profile	167
unconfig vlan ipaddress	71
unconfig inline-power priority	101
upload configuration	31, 177, 181
upload configuration cancel	177, 181
use configuration	176, 182
use image	182